Polynomial and Irrational Numbers



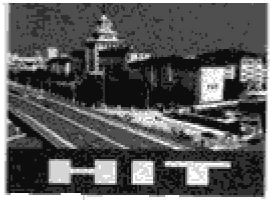
HIT

数学·统计学系列

多项式和无理数

冯贝叶　著

哈尔滨工业大学出版社
HARBIN INSTITUTE OF TECHNOLOGY PRESS



数学·统计学系列

多项式和无理数

冯贝叶 著

哈尔滨工业大学出版社
HARBIN INSTITUTE OF TECHNOLOGY PRESS

内容提要

本书从数的起源讲起，逐步介绍数的发展和新的各种性质及其应用，其中也包括了数学分析、实变函数和高等代数的一些入门知识，最后介绍了几个尚未解决的具有挑战性的问题。本书写法简明易懂，叙述尽量详细，适合于高中以上文化程度的学生，教师，数学爱好者以及数论、常微分方程、分支、混沌问题和 $3x+1$ 问题的研究者和有关方面的专家参考使用。

图书在版编目(CIP)数据

多项式和无理数/冯贝叶著．—哈尔滨：哈尔滨工业大学出版社，2008.1

ISBN 978-7-5603-2385-5

Ⅰ．多…　Ⅱ．冯…　Ⅲ．①多项式②无理数　Ⅳ．0174.14 0122

中国版本图书馆 CIP 数据核字(2007)第 175542 号

策划编辑　刘培杰　张　荣
责任编辑　李广鑫
封面设计　卞秉利
出版发行　哈尔滨工业大学出版社
社　　址　哈尔滨市南岗区复华四道街 10 号　邮编 150006
传　　真　0451－86414749
网　　址　http://hitpress.hit.edu.cn
印　　刷　黑龙江省教育厅印刷厂
开　　本　787mm×1092mm　1/16　印张 40.25　字数 742 千字
版　　次　2008 年 1 月第 1 版　2008 年 1 月第 1 次印刷
书　　号　ISBN 978-7-5603-2385-5
印　　数　1～3 000 册
定　　价　68.00 元

（如因印装质量问题影响阅读，我社负责调换）

前言

作者从年轻时就对整数的奇妙性质和有关整数的各种有趣问题十分感兴趣，后来随着数学知识的增加，才知道整数又可发展成为有理数、实数和复数，而各种数之间既存在着相互的联系，又有很大差别。而有关整数的问题，有时其解法不由得不令人拍案称奇。如此积累一多，发现如果不加整理和保存，很多精彩的想法就会擦肩而过。遂决定遇到有关的问题和材料就随时做一点笔记，到退休之时，竟积累了不少。这些笔记在多年的教学和辅导中，曾反复起了不少作用，因此觉得如把它们整理出来，对那些像我当年那样也对整数问题感兴趣的年轻人和初学者多少会有些帮助，于是就产生了这本书。

目前和本书内容及题材、体裁类似的书已有不少，其中也不乏广为人知的精彩作品。作者之所以还愿意写一本这样的书，是因为一方面，这些书有一些已难于买到和借到，另一方面是感到和已有的书相比，本书在以下几方面还是有一些新意和特色的，所以才敢不揣冒昧，班门弄斧。

(1) 一次不定方程是我国古代已研究的比较成熟和成就较多的一个课题，其中如孙子问题和孙子定理（又称中国剩余定理）已是世界数学界公认的成果。

以往介绍这方面内容的书不在少数，但是往往有的书把古代的算法讲得很清楚，其中的数学原理则让人不太明了；有的书

把现代的理论讲得很清楚,如何解释古代的算法则一笔带过。当我看到这些书时,对此总感到遗憾。本书将古代的算法和现代的理论一一加以对照,使读者可以很清楚地看出古代的算法其每一步的意义和依据是什么,尤其是秦九韶、黄宗宪等人创立的算法的最后一步,本书给予了严格的证明。

(2) 在复数得到了广泛的应用后,古代的数学家如哈密尔顿以及现代的初学者都曾思考过是否可以把复数推广为三元数。关于创立三元数的问题,许多科普读物都明确无误地告诉读者,这是不可能的,但是为什么不可能就语焉不详了。本书以比较浅显的方法对此作了论证。

(3) 费马大定理一直是几百年来数学家们和科普读物中的热门话题,虽然这一问题现在已经获得解决,但是人们对一些初等的证明还是十分感兴趣,其中比较难的一个是 $n=3$ 时的费马大定理的证明。一般的数论书籍通常只介绍 $n=4$ 时的费马大定理的证明,即使介绍 $n=3$ 时费马大定理的证明,也大都把它放在 $n=4$ 时的费马大定理的证明之后。这就足以说明 $n=3$ 时费马大定理的初等证明是有一定难度的。对这一比较难的问题,为使读者看懂,本应证明得更加详细,然而一些书在谈到这一问题时往往一开始就让读者看不下去了,其中最明显的一个地方是一开始就设 z 是偶数,很多人问过作者这个问题,后来经过作者反复钻研才发现在通常的 $x>0,y>0,z>0$ 的条件下是不能做这一假设的,只有在允许 x,y,z 可以是任意整数(即允许他们为负数)的条件下,才可以做这一假设。这一点在潘承洞、潘承彪先生的《初等数论》一书中交代得最清楚。本书对这一问题的证明力求详尽易懂,因此虽然篇幅长了一些,但是相信读者看起来会感到思路顺畅。

(4) 无理数小数部分的分布性质是无理数和有理数的一大本质差别,本书对此介绍得比较详细,并介绍了华东师范大学王金龙先生近年来获得的最新成果。

(5) 混沌理论是近年来的热门话题,本书用初等的方法证明了逻辑斯梯映射周期三窗口的出现参数和稳定的周期三轨道的消失参数。

(6) 关于多项式理论的应用,本书收集并重新证明了关于多项式系统的胡尔维茨判据和 Hopf(霍普夫)分支的代数判据。这些材料在一般的书中已不多见。

(7) 本书还给出了作者关于四次函数的根的完全判据和正定性条件,这些结果是有一定实用意义的可操作的判据,需要时应用这些结果还是比较方便的。

(8) 在整数的函数这一部分中,介绍了欧拉求和公式、贝努利数和戴德金和等概念,并证明了它们的相关性质。这些材料一般都分散在各种文献中,本书将它们收集在一起,对读者阅读本书和今后查找都是比较方便的。在这一部

分，还给出了一个数论中经常使用的不等式 $d_n<3^n$ 的初等证明，其中 d_n 表示前 n 个自然数的最小公倍数。

(9) 在本书第十二章中给出了几个著名的数的无理性和超越性的证明，其中包括法国数学家阿皮瑞 1978 年的最新结果——$\zeta(3)$无理性的证明。相信会有读者对这些材料感兴趣。

(10) 本书最后介绍了几个尚未解决的问题，其中包括著名的 $3x+1$ 问题，并给出了作者所获得的一些结果。还有一些结果在习题中给出，这些材料目前在其他书中还不多见。

本书在写法上尽量追求易懂性，为此，甚至不惜多费篇幅。这是因为当年作者在看某些书时，曾经因为有些地方被"卡住"而深感苦恼，所以作者特别能理解那种因各种原因而找不到人问以至心中的疑问长期不能获得解答的苦恼。为了避免本书再给读者造成这种苦恼，本书在讲解和证明时特别注意了这个问题，宁可显得啰嗦，也不愿语焉不详。从这个意义上来说，本书比较适合自学。

由于在讲解上不惜笔墨和追求材料的封闭性，所以目前本书的篇幅已不小。为了不再增加篇幅，有些材料就坚决舍去。例如，本书完全不包含有关素数以及素数分布方面的结果。关于特征和把一个整数表为平方和的方法的数目也都舍去了。在作者看来，这些材料太过专业，并不适合初学者阅读。当然有些作者认为从本书的体系看应该包含的材料也因为篇幅的原因不得不割爱了。例如，本书专有一章说明有理数性质和无理数性质之间的差别，而这种差别也可以从遍历论的观点得到反映，而不变测度等内容由于和连分数有关，因此适当介绍一些遍历论方面的基础知识似乎也是顺理成章的；然而，最终出于篇幅方面的考虑，作者还是不得不舍去了这方面的材料。这样一来，可以说，本书只包含了有关学科的最初等的材料，就数论方面来说，可以说是真正的初等数论了。

虽然本书舍去了不少材料，但是只要讲到的问题都争取讲透，因此，每一个问题几乎都会讲到最后完全解决，而不会使读者有虎头蛇尾的感觉。如果由于内容所限实在不能再讲下去，文中会特别声明。

本书包含了大量的习题，作者选取习题的用意是认为这些结果都是有一定趣味的和值得注意的，因此即使不知道答案也至少应该知道这些结果。

本书没有给出习题解答。这一方面是为了使读者永远有一种未知感以保持积极的思考，另一方面也在于本书的很多习题都取自书末的参考资料，特别是潘承洞、潘承彪先生的《初等数论》，杜德利的《基础数论》和北京大学数学力学系几何与代数教研室代数小组编写的《高等代数讲义》等书，而这些书中都有答案。当然有些习题是取自近期的《美国数学月刊》和作者的笔记，因而在其他参考文献中并没有现成的答案。

大部分习题的解答方法和所需的数学知识都与它所在的章节有关。然而，请读者不要受这一点说明的约束。这只是作者当初安排习题的动机之一，但是等全书写完之后，作者发现，有一些题目完全可以用另外的方法解出。所以，如果读者发现，他解题的方法似乎与这一题目所在的章节无关，请不要奇怪。这反而说明这位读者的思维是很灵活的。

至于最终是否会出一本本书的习题解答，还要看读者的反映。

最后，作者特别借此机会对教导过我的已过世的颜同照先生、闵嗣鹤教授、方企勤教授表示怀念，对孙增彪先生、叶予同先生、周民强教授、钱敏教授和朱照宣教授表示感谢，因为他们各位在做人、做事和做学问等方面给予我的教诲，都使我终身受益。

作者也对同事朱尧辰教授和同学王国义先生在讨论各种数学问题时给予的帮助表示感谢。

最后作者对妻张清真在生活方面的照顾，女冯南南在写作及计算机方面的帮助，弟冯方回在计算机方面的帮助以及他们对作者写作的理解和支持表示感谢。没有这些帮助，作者的写作将增加许多额外的困难，也不会有愉快的写作心境。

作者不是数论方面的专家，只是一个感兴趣者，因此殷切期望读者将本书的缺陷和不足之处反映给作者。有任何意见和建议请发电子邮件至 fby@amss.ac.cn.

冯贝叶

2007 年底于燕园 6 公寓

⊙目录

第一章　数是什么以及它是如何产生的？　//1

第二章　集合和对应　//12

2.1　集合及其运算　//12
2.2　有限集合的势　//16
2.3　无限集合的势　//26
2.4　不可数的集合　//33
2.5　无限集的势的比较　//35

第三章　整数的性质　//44

3.1　整数的顺序　//44
3.2　整数的整除性　//46
3.3　最大公因数和最小公倍数　//50
3.4　素数和算数基本定理　//60
3.5　方程式的整数解　//64
3.6　同余式　//81
3.7　欧拉定理和费马小定理　//97
3.8　整数的函数　//105
3.9　同余式的方程　//139

3.10　二次同余式　//167
3.11　原根和指数　//182

第四章　有理数的性质　//206

4.1　用小数表示有理数　//206
4.2　有理数的 10 进小数表示的特性　//213
4.3　循环小数的一个应用　//219
4.4　整系数多项式方程的有理根　//222
4.5　实数和极限　//228
4.6　开集和闭集　//236
4.7　隔离性和稠密性　//252

第五章　无理数　//262

5.1　无理数引起的震动和挑战　//262
5.2　一些初等函数值的无理性　//265
5.3　对称多项式　//269
5.4　代数数和超越数　//277

第六章　连分数　//283

6.1　什么是连分数　//283
6.2　用连分数表示数　//288
6.3　二次无理数和循环连分数　//294
6.4　连分数的应用 I：集合论中的一个定理　//306
6.5　连分数的应用 II：不定方程 $ax \pm by = c$ 的特解　//307
6.6　连分数的应用 III：Pell 方程　//308
6.7　连分数的应用 IV：把整数表为平方和　//319

第七章　用有理数逼近实数　//329

第八章　实数的光谱：小数部分的性质　//352

8.1　小数部分的分布　//353
8.2　殊途同归——有理数和无理数小数部分的一个共同性质　//367

第九章　复数　//381

9.1　复数及其几何意义　//381

9.2 复数的方根 //393
9.3 群、环和域 //398
9.4 整数的推广:各种复整数 //414
9.5 $n=3$ 时的费马问题 //431
9.6 复数的推广 //445

第十章 多项式 //455

10.1 多项式及其基本性质 //455
10.2 代数基本定理和多项式的唯一分解式 //459
10.3 重根和公根 //478

第十一章 多项式的应用 //488

11.1 动力系统奇点的线性稳定性的代数判据 //488
11.2 和 Hopf 分支有关的代数判据 //499
11.3 插值多项式和最小二乘法 //505
11.4 Logistic 映射周期 3 窗口的参数 //522
11.5 三次方程的解法和判据 //535
11.6 四次多项式零点的完全判据和正定性条件 //544

第十二章 几个著名的数的无理性和超越性 //561

12.1 勒让德多项式和它的性质 //561
12.2 e 的无理性 //567
12.3 π 的无理性 //568
12.4 ln 2 的无理性 //572
12.5 ζ(2)的无理性 //573
12.6 最新的记录:ζ(3)的无理性 //581
12.7 e 的超越性 //586
12.8 π 的超越性 //589

第十三章 数的挑战仍在继续:几个公开问题 //593

13.1 ζ(5),ζ(7),…是有理数还是无理数 //593
13.2 欧拉常数 γ 是有理数还是无理数 //595
13.3 $3x+1$ 问题 //602

参考文献 //622

冯贝叶发表论文专著一览 //627

编辑手记 //631

数是什么以及它是如何产生的?

第一章

我们每个人每天大到工作需要,小到买菜算账都要和数字打交道,但是对于数究竟是什么以及它是如何产生的这些问题,恐怕不是每个人都想过的。其实认真地思考一下这个问题就会发现如果你的数学课学得不错的话,那么你其实已具有了很了不起的本领了,尽管你自己并不一定意识到。

人类是从动物进化来的,能够感觉到客观世界中某种同类事物的数量是某些动物的一种本能。比如有的鸟类能够发现自己鸟窝中的鸟蛋少了,哺乳类动物也能发现自己生下的幼崽少了,这恐怕就是最初级的识别数量的能力了。也有证据表明一些比较聪明的动物已经不仅能识别事物的多和少,对一定数量之内(比如说,3个以内或5个以内)的物体还能具体分辨出究竟有多少个。但是动物对于数量的感觉恐怕也就到此为止了,数量一多,它们就分辨不清了(至多有一种多的感觉),对于数的更深刻性质就更谈不上有感觉了。中国有一句成语叫"朝三暮四"就相当准确地反映了即使是进化已经比较高级的动物对于数量的感觉。《庄子·齐物论》中说有个人养了一群猴子,他对猴子说,早上给每个猴子三个橡子,晚上给四个,猴子都不干,很生气,结果他又说,那好我早上给四个,晚上给三个,结果猴子就都高兴了。这说明猴子对于数量有感觉,而且已经能分辨到四了,但是猴子不懂加法交换律。

其实我们人类一开始也比动物好不了多少。我这里说的一开始是指早期的人类和人类自身成长的一开始。那么我们怎么知道人类的一开始对数的概念的认识程度呢?原来进化论的研究告诉我们,人的胚胎的发育过程就浓缩了人的进化过程,而人诞生后的婴儿时期也浓缩了人类的智力发展过程,同时现存的一些处于封闭环境中的原始部落也可让我们知道早期人类的智力程度。

有不少非洲探险家证实,在某些原始部落里,不存在比3大的数词。如果问一个人他有几个儿子,或杀死过多少敌人,而这个数字大于3,他就只会回答“许多个”,因此,要说数数(第一个数念 shǔ,第二个数念 shù)这个本事,这些部落的勇士们甚至还不如我们幼儿园里的小朋友呢,因为这些小朋友都可以从一数到十。

但是为什么幼儿园中的小朋友都会从一数到十呢?那是因为有大人从小就教他们。如果情况不是这样,那么他们的命运就不同了。据文献记载,从小被狼攫取并由狼抚育起来的人类幼童,世界上已知的狼孩已有10多个,其中最有名的是印度发现的两个。1920年,在印度加尔各答东北部的一个山村附近,居民们常在傍晚时分看见一头母狼走出山林,后面跟着两个似人非人、似狼非狼的怪物。为了弄清事情的真相,人们伺机把母狼打死,在狼窝里发现那两个怪物原来是两个女孩,于是人们把她俩抱回到村子里。大女孩估计有七八岁,给她取名叫卡玛拉;小女孩大约两岁左右,取名阿玛拉。

卡玛拉和阿玛拉被人们从狼窝中救出来以后,由米德纳波尔孤儿院收养。这两个女孩的行为方式和生活习惯同狼一样,不会说话,没有人的思想意识,也没有人的复杂和丰富的情感。走路时四肢着地,坐卧如犬状。饥餐渴饮像狗那样趴在地上舔食,活动规律呈昼伏夜出的特点,白天吃饱了就睡。饿了就引颈长嚎。夜晚来临时即表现得躁动不安,因为不能随意到旷野里去,便在黑暗中于室内或院子里来回游荡,并又东闻西嗅地寻找可食之物,时时刻刻总想出逃。给她们穿衣或围上腰布,她俩便粗野地撕扯下来。

在这两个狼孩刚回到人的周围时,她们的智力只相当于初生婴儿的水平。在孤儿院里将近一年的生活期间,她俩皆未改变自己身上原有的那种狼的习性。大狼孩卡玛拉在进入孤儿院的第二年里,仍然寻食死鸡的内脏,第三年里依旧在晚上东游西荡,大声嚎叫,寻机逃跑。小狼孩阿玛拉由于染患重病,在孤儿院里生活了11个月便死去了。而卡玛拉却在以后将近9年的时间里,受到了精心的照料和培养。

为了帮助卡玛拉尽快恢复人性,有关人员对她进行了各种教育尝试,以促其早日学会人的生活。但是学习对于这个女孩来讲,是相当艰难和困苦的事,很少有所收获。每一少许的进步,都需要教养人员花费特别大的代价。比如教她说话,仅教她呼唤照料她的波拉夫人的“波”字发音,她就足足用了两年的时间才

勉强算是学会。后来又教她说些简单的词句,6个单词她用了4年的学习时间。经过7年的教育,她一共学会使用45个单词。教她直立行走也很困难,在有关人员的耐心示范和训练下,她用了1年零4个月的时间学会用两膝行走,花了2年7个月的时间学会两腿站立,大约经历5年的努力才学会用两脚步行,而且很不习惯,每当需要快速行走时,她仍喜欢用四肢着地而行。

尽管如此,回到人类中的卡玛拉经过几年的教育和训练,还是开始改变她初时狼的生活习性,并逐步适应人类的社会生活。在进入孤儿院第4年以后,卡玛拉的智力发展已达到一岁半幼儿的水平。从此以后,她的心理和行为变化较前几年有了显著的进步和提高,到第7年的时候,她的生活习惯同其他孩子相比已相差无几。例如她也像其他孩子一样注意自己的穿着,并以自己整洁漂亮的服装而高兴。同时也产生了羞耻心,穿衣系带不愿接受别人的帮助,常因自己动作缓慢而感到焦急。她还希望得到别人的夸奖,一次由于她及时地报告了一个婴儿发生的一点问题而受到称赞,她兴奋得两眼闪出喜悦的光芒。她能知晓一些简单的数目,拒绝接纳多于定量的饼干或点心。后来因为身患重病而死亡。死时年龄大约17岁。据心理学家对她死前心理活动状态及社会行为表现确认,她的智力已达到三岁半幼儿的水平。如果她能继续活下去的话,可以断定她的智力还会得到发展和提高。

这就说明,即使我们的大脑已经具有了接受现代知识的结构,但是如果不生活在现代环境中和接受教育,那么我们的智力也只能停留在很原始的程度。

现在我们可以回答数是怎样产生的这个问题了。数(shù)是产生于数(shǔ)。最开始,人们会数1,然后是2,再然后是3,… 并且发明了表示这些数字的符号。下面分别是是1 ~ 10的汉字、罗马数字和阿拉伯数字的符号:

一,二,三,四,五,六,七,八,九,十
I, II, III, IV, V, VI, VII, VIII, IX, X
1, 2, 3, 4, 5, 6, 7, 8, 9, 10

实际上,罗马数字的表示法还更复杂,在这个体系中,首先用以下符号表示几个特殊的数字:

I, V, X, L, C, D, M
1, 5, 10, 50, 100, 500, 1000

把I,II,III,放在V和X的左边就表示从V和X分别减去I,II和III,而把它们放在右边,就表示从V和X分别加上I,II和III。于是十、十一等数即可以分别写成

X, XI, XII, XIII, XIV, XV…

二十,三十则写成XX,XXX。

要表示四十及四十以上的数，就要利用符号 L。例如四十一写成 XLI(即五十减去十加上一)。九十就要利用符号 C 来表示，即写成 XC，另外 49 和 99 并不写成 XLIX 和 XCIX，而是写成 IL 和 IC。一百零二写成 CII，三百七十四写成 CCCLXXIV 等等。大的数，如 29 635 写成 XXIXmDCXXXV(小写字母 m 表示千，即 29 个千加上 500，再加上 100，再加上 35)。数字的这种记法很经济(只用七个数字就可写出一百万以内的数)，但却不方便。因为不太大的数就要写得很长，而计算时并不能得到任何便利。用汉字来进行计算也不是很方便，因为毕竟笔画较多，书写不如阿拉伯数字流利，因此目前世界上通用阿拉伯数字来记数和进行笔算。(虽然用汉字表示的数字在计算方面并没有什么优越性，但是我们的祖先却发明了算盘，这一简易的计算工具由于其实用性，一直流传到现在。) 不过由于阿拉伯数字容易被改写或辨认不清，因此各国在比较正式的经济活动中和票据中还要对数字使用所谓的大写来表示郑重和正式。下面是汉字中，数字 1 ~ 10 的大写：

壹，贰，叁，肆，伍，陆，柒，捌，玖，拾

比如人民币 36 745.12 元用大写就要写成叁万陆仟柒佰肆拾伍圆壹角贰分；而在英语中，英镑 36 745.12pound 用大写就要写成 thirty - six thousand，seven hundred and forty - five point one two pounds 或 thirty - sixthousand，seven hundred and forty - five pounds and twelvepennies。人民币 21 536 745.12 元用大写就要写成贰仟壹佰伍拾叁万陆仟柒佰肆拾伍圆壹角贰分；而在英语中，同样数目的英镑数用大写就要写成 twenty - one million，five hundred and thirty - six thousand，seven hundred and forty - five point one two pounds 或 twenty - one million，five hundred and thirty - six thousand，seven hundred and forty - five pounds and twelve pennies。怎么样，朋友？你可能对数字不感兴趣，但无论如何，你是离不开数字的。如果你发了财或出国了，可是却连一张支票都写不成，那可是有点尴尬哦！

一旦把数字用一种符号表示出来，人类就完成了一次认识上的飞跃，因为数字 1 已经是一个抽象的概念了，它既可以表示一个人，也可以表示一头牛或是任何数量是一的对象。数字的抽象概念就极大地延伸了它的作用，因为从此之后，人类在进行计算时就再也不用去考虑数字所代表的各种具体对象的与数字无关的性质，而只要考虑数字本身的性质就行了。

另外有了最基本的数字 1 之后，通过合并两个 1 就可以产生 2，再把 2 和 1 合并就可以产生数字 3，原则上，这个过程可以无限地进行下去。正如中国的一部名著，老子的《道德经》中所说的："道生一，一生二，二生三，三生万物。" 这就是人类思维上的又一次飞跃，就是从有限到无限的飞跃。原则上，我可以想象要多大就多大的数的存在，这只要把 1 这个数无限次地相加下去就可以得到，但是在实际操作中，我们又不可能无限次地相加，所以无限这一概念只能通过抽象

的思维来认识。

这就又产生了一个矛盾或问题，即如何来表示这无限多个数字的问题。显然，对每一个数字给予一个特别的符号是一种无法实现的方案。有一个民间故事反映了这一问题。据说有一个姓万的财主特别吝啬，给他儿子请了一个教书先生。先生教了一天后，财主问他的儿子，今天学了什么字，儿子说，今天我学会写“一”字了，第二天说我学会写“二”字了，第三天说我学会写“三”字了。这个财主一看，学字也不难啊，一个字多一划，以后肯定也差不多。学这几个字也就够用了。没必要花那么多冤枉钱请先生。结果就把先生给辞了。过了几个月，这位财主准备为儿子过生日请一次客，同时也趁机显示一下自己的儿子会写字了。就让他的儿子在请帖上代他签字。结果过了一天，这个财主来问儿子名字签完了没有，儿子说：“爹呀，还早着呢，光你这个姓就要划一万道，现在我才划了几百道。”其实这个财主的儿子还不算笨，不但数数得清，而且对没有学过的数字还能用类推的办法给出一个表示的方案，只不过这个方案无法实现罢了。（其实罗马计数法也不比这个财主的儿子高明多少，如果要写一个很大的数，比如说一百万，罗马人所能使用的最好的办法，就是接连不断地写上一千个 M，这虽然用不了一天，却也得花费好几个钟头。）

各个不同的文明，如巴比伦、印度和中国都各自独立地发明了进位法，用这种方法，我们就能用有限多的符号表示无限多的数字。最常用的进位法是十进制，而且各个不同的文明几乎不约而同地都产生了十进制的计数法。这大概不是偶然的。有的专家认为，这可能和人类最初是借助于手指来计数(想一下儿童最初是如何数数的)，而与我们的双手一共有十个手指有关，的确，我们的双手就是一个天然的十以内的计算器。当然除了十进制之外，还有其他的进位制。例如在中国的重量计量中，采用 16 进位制，在计算时间时，我们又采取 60 进位制。

但是即使有了进位制，我们在表示很大的数时，原则上仍要发明无限多的单位，而刚才已说过，这是不现实的。大概在两千年之前，一位不知名的印度数学家发明了一种表示数的方法，这种方法可以使我们写出任意大的数字。例如目前可以观测到的宇宙中所有原子的数目约为 300 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 个，这个数字要让你念出来恐怕都很困难，因为没有那么大的单位。但是用那位不知名的印度数学家发明的办法，这一数字就可以写得很短，即写成

$$3\times 10^{74}$$

这里，10 的右上角的小号数字 74 表示 3 后面有 74 个零，即要 10 自乘 74 次再去乘 3。用这种方法，我们就可以表示出任意大的数。例如，下面是一些物理常数：

地球的半径：6 37 1 km；

地球的质量：5.98×10^{27} g;

太阳的质量：2×10^{33} g;

月球的半径：1 740 km;

月球的质量：7.35×10^{25} g;

下面是一则关于发现最大质数的新闻报道：

美国州立中密苏里大学的一个团队利用700多台计算机通过分布式运算发现了迄今为止最大的质数，一个9 152 052位的天文数字。这一数字是在2005年12月15日被发现的，并已得到了确认。

他们发现的这个900多万位的数字是第43个梅森质数，为 $2^{30\,402\,457}-1$。

由此可见，这种表示数字的方法现在已深入到我们的生活中。在上面的表示法中，我们已见过数字零。发明和使用数字零也是人类认识上的一次飞跃。零可以表示没有，同时使用数字零可以使我们区分像12，120，102这些不同的数字，零的使用极大地方便了我们的思维和计算，在我们的生活中，如果没有零这个数字，那将是不可想象的。

零和数字1，2，3，… 的全体已经组成了一个有着很好性质的计算整体，现在我们把零和数字1，2，3，… 的全体称为(非负) 整数。例如在这些数中可以进行两种运算，即加法和乘法，而且这两种运算还服从以下5个规律：

加法交换律 $a+b=b+a$

加法结合律 $a+(b+c)=(a+b)+c$

乘法交换律 $ab=ba$

乘法结合律 $a(bc)=(ab)c$

乘法分配律 $a(b+c)=ab+ac$

$$(b+c)a=ab+ac$$

次序关系：对任意的 a,b，三个关系式 $a>b$，$a=b$，$a<b$ 之中，必有一个成立，且其他两个关系式不能同时成立，其中 a,b 是0或正整数；

$$1>0$$

$$a>0,b>0 \Rightarrow a+b>0$$

$$a>0,b>0 \Rightarrow ab>0$$

$$a>b,b>c \Rightarrow a>c，其中\ a,b,c\ 是0或正整数$$

(由于成立加法和乘法的交换律，所以乘法分配律中的两个式子实质上是一个式子。)

其实在整数范围中，乘法的地位没有加法那么基本，它是作为加法的简便算法而出现的，但是它一旦出现后，就有了独立性，而在数的范围扩大后，它就完全脱离了加法而独立了，因为在扩大的数中，乘法已完全不能用加法的简便运算来解释了。但是注意到乘法的起源还是有助于我们理解为什么乘法也遵循

与加法完全相同的运算规律，并且与加法协调得如此和谐，因为它本来就来源于加法。而且思考一下以下问题也会让我们感觉到这两种运算的基本重要性。就是尽管我们还可以模仿乘法而定义什么其他的简便算法，但是这些算法最终都可以归结到加法和乘法，所以至今我们的小学算术只须背诵九九表（也就是乘法运算表）就到头了，而不需再背诵什么其他的运算表了。而去掉了加法或乘法任何一种运算，我们就什么计算也无法完成了。

但是从实用的观点来看，光有整数是完全不够用的。因为在客观世界中存在着两种性质完全不同的对象。一种对象是完整的，不可分割的。即如果你把这种对象加以分割，它就已不再是它本来的样子了。再说得具体一些，例如一个人、一头牛、一只箭、一个盘子、一个瓶子等等，都是不能分割的对象，把这些对象分成哪怕仅仅是两半，它们就不再是人、牛、箭、盘子、瓶子等原来意义上的东西了。整数就是用来计数和计算这种不可分割的对象的。然而还有另一种对象，即连续的和均匀的量，这种对象既容易分开来也容易结合起来，而不失去它们原有的本性。例如长度、面积、体积还有时间都具有这样的性质，我们把这种性质称为连续性。连续性这一概念的本质就是所说的对象虽然实际上还没有被分割，但是潜在上却具有无限分割的可能性。要反映和计算这种量，光有整数是不够的，也就是说，必须对数的概念进行扩充。在人类的认识史上，这种扩充进行过不止一次。

数的第一次扩充来源于数的另一起源，即度量。从这个观点来看，数就是用叫做单位的量去度量同类的量的结果。当社会发展到需要对财产、战利品、土地的面积、物体的体积以及时间（因为和时间有关的历法是和农业紧密相关的，而农业长期以来是人类最基本的和最重要的生产形式之一）进行精确度量时，数就必然产生了。用度量的方法不仅能产生整数，而且必然产生分数。所以用度量方式产生的数包括了用数的方式产生的数。世界上几个比较重要的文明起源地，如古希腊、印度、埃及都在其文明发展的早期就已认识了分数。我们中国也是世界上一个重要的文明起源地，而且很重视数学的实用。因此中国人也很早就掌握了分数的实际应用。例如《管子》是春秋初期著名的政治家、军事家、经济学家、哲学家和音乐家所著的一本先秦时独成一家之言的最大的一部杂家著作。其中的地员篇里讨论音乐。说把发“宫”音的管子的长度“三分而益之以一”便得到能发“徵”音的管子的长度。另外一本在公元前三世纪左右写成的“考工记”在讲到制造车轮时，也有“六分其轮崇，以其一为之牙围”“参分牙围而漆其二”等说法。可见我们中国人远在秦朝以前，就已经能掌握分数的实际应用了。

《九章算术》是一本秦汉数百年间数学研究成果的总结性著作。其中有大量和分数有关的问题，例如有一个问题是：今有凫从南海起飞，7 日可到北海；雁从北海起飞，9 日可到南海。今凫雁同时起飞，问经几日相遇？其答案就是一

个分数。还有一个问题是：今有人持米出三关，过内关时纳税七分之一，过中关时纳税五分之一，过外关时纳税三分之一。出三关后剩米五斗，问原持米多少？这里不但答案是分数，而且问题的条件中就已有分数。

另一本大约完成于西汉末年的数学书籍《周髀算经》中关于月行速度的计算也使用了分数的运算。

有了十进制和分数，小数也就自然而然地产生了。但是我们的祖先似乎并不偏爱使用这种形式。虽然他们实质上已经有了这一概念，但是他们就像表示大的数字一样，宁愿使用像丝、毫、微等具体的单位，尽管这样表示一个很小的数并不方便。在表示一个很小的数时，上面提到的那位不知名的印度数学家发明的方法同样是很有效的。下面是一些很小的数：

电子的静止质量 $m_e = 9.106 \times 10^{-28}$ g

中子的静止质量 $m_n = 1.675 \times 10^{-24}$ g

质子的静止质量 $m_p = 1.672\,5 \times 10^{-24}$ g

氢原子的质量 $m_H = 1.673\,4 \times 10^{-24}$ g

就像上面我们考察乘法那样，注意到乘法的起源，我们就能够"预见"或至少理解、感觉到乘法应有哪些性质或乘法的性质是从何而来的。同样，考察分数的起源，也能使我们能够"预见"或至少理解、感觉到分数应有哪些性质或分数的性质是从何而来的。如果允许分数的分母和分子取任意的数，那么分数只不过是除法的另一种写法而已。因此我们只考虑分子分母都是整数的分数，这样一来，分数的所有运算最终都归结为整数的运算，而且如果我们取一个适当的量作单位(具体地说，这个量就是这些分数的分母的最小公倍数的倒数)，(注意，单位是可以改变的。例如，我们数鸡蛋时有时一对一对地数，这就是用 2 作新的单位。选举基层干部时，常在前面的黑板上，够了 5 个人就写一个"正"字，这就是用 5 作新的单位。商业中还有用"打"计数的，这就是用 12 作单位。单位变了以后，度量出来的数也会改变，物理学中经常需要把同一个量用不同的单位表示，并在这些用不同单位表示的数字之间进行换算。这种换算的公式是：在新单位下度量出来的数等于用原单位度量出来的数除以新单位。比如要把 2 尺 7 寸换算成米，那么新的单位就是米，而 1 米等于 3 尺，按照上面的公式，我们应该用 2 尺 7 寸即 2.7 尺去除以新的单位即 3 尺，写出来就是 $2.7/3 = 0.9$，因此 2 尺 7 寸 = 0.9 米)，那么有限个分数就可以同时成为整数(即同时成为这个单位的整数倍)。因此我们有很大的把握期望分数应与整数一样遵循同样的运算规律，事实上也正是这样。分数无疑是比整数更为复杂的对象，因为它由两个整数组成。而且存在着形式上完全不同的无穷多的分数，而实际上它们都代表同一个分数(例如二分之一，四分之二，六分之三，… 实际上都只是一个分数)，从这一事实出发，可以发展出像等价、商空间等近代的观念。这里我们看到了这样的

情况，就是我们扩大了数的范围，但是新的更复杂的对象和原来的对象有很好的协调关系。以后我们会不止一次地看到，这一原则是我们不断扩充数的概念时始终想保持的，除非到万不得已的时候，我们是不愿意放弃这一原则的。

有了零、正整数和正分数之后，从实用的观点来看，我们就可以完成一切实用的计算需要。的确，即使在今天这样数学已高度发达并系统化的时代，我们的一切实用的计算，最后仍归结到只须用到这些数就够了。所以对于一般人来说，始终不会感到如果不再增添什么新的数会有什么不便。但是科学的发展动力，从它出现的那天起，就不只是因为要解决实际中的具体问题，科学发展的另一个动力还来自它要解决内部的自我协调性所提出的问题。科学研究发现客观规律的过程有时看起来就像研究者在玩一个神秘的拼图游戏，来自不同领域的发现或概念都会以令人惊讶的程度互相吻合和衔接、协调。数学也是这样，当我们在处理数学内部出现的问题时，我们自然会产生这样一种倾向，即使用尽可能统一的原则和规则。

这就是数要进行扩充的另一个起源。上面已经讲到，在零、正整数和正分数之间可以进行加法和乘法两种运算。出现了一种运算后无论是实际问题还是理论本身必然会提出如何做逆运算的问题。比如，加法是已知两个加数 a，b 求他们的和 c，而问题有时是已知一个加数 a 和他们的和 c，求另一个加数 b。这就归结到一个方程 $a + x = c$。如果只限于正数，这一方程就可能没有解。同样形式的方程，有的有解，有的没有解，会使人们在研究它们时感到极大的不便，仅仅在研究使用的语言上就会使你不胜其烦。所以数学家希望这些方程都有解，哪怕是形式上的解。企图使方程有解这一动机就导致了负数、无理数，乃至复数的产生。这就是数的第三个起源。复数产生之后又产生了四元数、八元数。但是到目前为止，数的扩充到复数为止已经完备(也就是说，没有必要再进一步进行扩充了)。而数的这几次扩充每一次都造成了一部分人认识上的危机和矛盾。而这几次危机又是促进数学向前发展的重大动力。

比如说，就像分数刚出现时那样，有人就要问，二分之一个人是什么意思？对此，我们的回答是二分之一个人的确是没有意义的，但是，这不能用来说明，二分之一这个概念是没有意义的，因为存在着用二分之一表示而有意义的量，例如二分之一亩地，二分之一秒等等。负数刚出现时，也有人要问，-1 个人，-1 亩地是什么意思，对此问题的回答与上面是类似的。的确，抽象地说 -1 个人，-1 亩地是没有意义的，但是这不能用来说明，-1 这个概念是没有意义的，因为存在着用 -1 表示而有意义的量，例如 -1 摄氏度就表示摄氏零下 1 度。何况 -1 个人，-1 亩地如果联系到一定的具体的问题就可能产生意义，例如，它可以表示少一个人少一亩地。当然，也可能存在着无论怎样解释用 -1 表示都没有意义的量，但是刚才我们已经说过，即使存在着这种量，也不能用来说明

-1 这个概念是没有意义的。

还可以从另一个方面来说明负数产生的必要性，即即使是完全从形式上引进负数，也会在实用上产生极大的便利。

例如，如果没有负数，加减法混合运算就必须遵循被减数大于减数的原则，这样一来，我们就不能任意交换运算的次序，而 $1-2+3-4+5-5+4-3+2-1$ 甚至从一开始就不能够进行下去。

例如，如果没有负数，要表示一条直线上 3 个点 A,B,C 所产生的各个线段之间的长度关系，就必须讨论以下 6 种情况

$AB+BC=AC$（A 在 C 左边，B 在 A,C 中间）

$AC+CB=AB$（A 在 B 左边，C 在 A,B 中间）

$BA+AC=BC$（B 在 C 左边，A 在 B,C 中间）

$BC+CA=BA$（B 在 A 左边，C 在 B,A 中间）

$CA+AB=CB$（C 在 B 左边，A 在 C,B 中间）

$CB+BA=CA$（C 在 A 左边，B 在 C,A 中间）

这还不包括这 3 个点中有某几个点重合的情况，而如果规定，线段的长度从左向右用整数表示，而从右向左用负数表示，则任何情况下（包括以上 6 种情况和有某几个点重合的情况），各个线段之间的长度关系就可以用一个统一的式子 $AB+BC=AC$ 来表示。

例如，如果没有负数，甚至平面解析几何都无法产生，因为我们只能表示第一象限的点。然而整条的直线，在各个象限都能延伸的几何图形却是一种客观存在的对象，它不会因为你无法表示而不存在。也许，有人能发展出一套不用负数的系统来处理这些事情（我不知道是否能够发展出这种系统，但如果你仅仅使用另一个名词，而实际上仍是负数的东西来解决问题，那只不过是一种自欺欺人的方案），但正像我们刚才表明的那样，这种体系必然是一种语言极其繁琐，手段上自找麻烦的体系，而一旦有人引进负数，而使得同样的问题可以更为简便地解决（你无权阻挠别人使用负数）时，所有的人都会感到，干吗要绕那么大的圈子，就会抛弃那个体系而接受负数（除非那种体系是像中世纪的教会那样以权利维持它的学说，不过即使那样，它遭到被抛弃的命运也只是时间问题）。如果没有负数，行列式的理论也无法产生，整个高等代数，现代的数学分析即整个的现代数学都无法产生，那我们就只能永远生活在蒙昧时代。

从最简单的整数 1 产生算起，到复数的产生，人类用了几千年的时间。而这些知识现在的人只须学习十几年就能掌握。如果你的数学课学得不错的话，你已掌握了古代人要几千年之后才能知道的奥妙和技巧，所以在古代人的眼里你其实已具有很了不起的本领了。设想一下如果你突然回到古代会怎么样？事实上，已经有不少人设想过这种场面。按照某些人的设想，通过一种叫做时间隧道

的通道，你就能够回到古代，甚至能够再见到你的祖先，而那些人因为你具有神奇的本领将把你视为神仙，待若上宾。好像有一本叫《从月亮上来的人》的书就设想过一个现代人因为海难，漂流到一个只有未开化部落的岛上，他随身带了一只箱子，里面装有酒精等物，上岛之后，他对当地土人表演了他的神奇本领，一是可以使水着火（其实是用火柴把酒精点燃），结果是当地人非常恐怖，乞求他不要把他们赖以生存的宝贵的水烧掉。二是他根据天文知识，知道哪一天会发生月食，结果他预言那一天天狗将会吃掉月亮，又引起了一场恐慌，他当然知道月食会过去，所以答应帮他们把天狗赶走。这又使当地人对他感激零涕，把最好的食物送给他。怎么样，是不是很美妙？不过且慢，因为这种设想还包含着另外一种可能性。就是有着特殊能力的人在古代既可能被视为神仙，也可能被视为魔鬼和巫术。如果你被看成魔鬼和巫术那结果可并不美妙，况且，在有的部落中，先不管你有没有什么本领，而首先把你视作一道可口美味的大餐，如果这样，可就更有点恐怖了。更何况，古代的人在有些方面已经达到了不可想象的高度，他们所能解决的问题即使是现代也不是每个人都能够解决的。比如说，阿基米得的国王让他解决的问题你是不是能解决呢？传说公元前叙拉古国王海隆命令金工替他打造一只纯金的王冠。不久，金工就把王冠打造好了。王冠金光灿烂，国王见了非常高兴和喜欢，打算重重地赏赐匠人。但是正在这时，有人对国王说，金工在制造时有可能揩了一点油，在王冠里掺了一点银子，这就贬损了它的价值。国王一听觉得很有道理。因此就想知道这顶王冠到底掺了银子没有。但是他又非常喜欢这顶王冠的样式，因此又规定无论什么人检验时都不允许把这顶王冠损坏一丝一毫。结果朝中的大臣们都感到国王的条件太苛刻，无法应命。国王海隆看见他的臣子这么不中用，极为烦恼。最后他想到了他的顾问，国内最聪明的人阿基米得，决定把这件事交给他办理。据说阿基米得也是苦苦思索了很久才解决这一问题的。阿基米得还会求抛物线和它的弦围成的面积。这些问题你都能解决吗？国王海隆还算是比较开明的，对于解决不了他的问题的大臣也就是烦恼而已，有的国王或皇帝可就不那么好说话了，他们的问题解决不了可是要杀头的。所以还是就呆在现代，好好地学习，学得一身好本领，好好地工作，好好地生活吧！

集合和对应

第二章

2.1　集合及其运算

集合这个概念其实是非常直观的，不管你是否意识到，实际上在人们的潜意识中都会使用这个概念，比如当你在说所有这个词时，你很可能就在运用这个概念了，因此这是数学中的一个原始的无法再定义的概念了。但是近代的基础研究又发现，这又是一个很复杂的概念，如果不适当地扩大它的适用范围，就将会引起使我们的整个数学基础崩溃的危机。在本书中，不讨论与此有关的基础问题，只给出集合的朴素直观的描写。并在不致引起矛盾的合理范围内使用这一概念。

凡是具有某种特殊性质的对象的全体就称为一个集合。例如全体自然数的集合，直线上所有的点的集合，全体整系数多项式的集合等等。任给一个对象 x 和一个集合 A，则 x 或是属于 A，或是不属于 A，但是不可能 x 既属于 A 又不属于 A。

如果 x 属于 A，则记为 $x \in A$。

如果 x 不属于 A，则记为 $x \notin A$ 或 $\overline{\in} A$。

我们规定，一个集合本身不能作为这个集合的元素（这与我们刚才提到的不适当的扩大集合的适用范围会引起数学基础中的矛盾问题有关），也就是规定对任何集合 A 有

$$A \notin A$$

实际上，这一规定也非常直观。可以把集合比做一个大口袋，在没有定义一个集合之前，这一口袋并不存在，当我们定义一个集合之后，就产生了一个新的对象，那就是包含集合中所有元素的口袋。这个口袋中的东西就是集合的元素，但是这个口袋不能把自己也装进去。你可以用另一个口袋来装这个口袋，但是一个口袋自己不能装自己。

为方便起见，我们引入空集的概念，就是不含任何元素的集合。如果通过上下文的呼应不会引起误解，我们有时就用 0 来代表空集，有时也用∅来代表空集。

有时也会遇到由单个元素组成的集合，即单元素集。这时要注意，不要把单元素集和这个集合所包含的单个元素混起来。（从下面的例子中可以看出二者是不一样的）

现在来说一下如何表示一个集合。

最简单的表示法是所谓列举法，就是把集合中的元素列举出来，这时可先将集合中的元素列举出来，然后再在它们外面加上一个花括弧。例如

$$A = \{a, b, c\}$$

全体正整数的集合可以表示成

$$N = \{1, 2, 3, \cdots\}$$

等等。注意，用列举法表示集合时，每个元素只须写一次，而且不考虑顺序。但是这种方法对有的集合不适用。例如有的集合中的元素不可能一一列举出来，或即使列举出来了，其规律并不明显，除了列举人自己心中明白，其他人仍然无法知道。因此更经常使用的方法是所谓描述法。用描述法定义集合的写法是在花括弧中的左边写上代表集合元素的符号，然后在其右边画一条竖线，在竖线右边用语言或公式写出集合元素所满足的特性。例如

$$A = \{x \mid x^2 - 5x + 6 = 0\}$$

$$M = \{(x, y) \mid x, y \text{ 都是整数}\}$$

等等。

定义 2.1.1　若集合 A 的所有元素都是集合 B 的元素，则称 A 为 B 的子集，记为

$$A \subset B \text{ 或 } B \supset A$$

这时 B 称为 A 的包含集。

设 A 是任意一个集合。显然有 $A \subset A$ 和 $\varnothing \subset A$。后者之所以成立是由于一个命题和它的逆否命题是等价的。把子集定义中的话换成它的逆否命题就得到 $A \subset B$ 的含义是如果一个元素不属于 B，则它也不属于 A。如果集合 A 与集合 B 表示同一个集合，则称集合 A 与集合 B 恒同，记为 $A = B$。根据上面的说明和恒

同的定义就有如果 $A = B$,则有 $A \subset B$,同时有 $B \subset A$。由恒同的定义得出,A,B 不相同(记为 $A \neq B$) 的意思即是至少存在一个元素 x 使得 x 属于 A 而不属于 B,或至少存在一个元素 x 使得 x 属于 B 而不属于 A,因此包含关系 $A \subset B$ 和 $B \subset A$ 不可能同时成立。这就是说如果 $A \subset B$,同时 $B \subset A$,则必有 $A = B$。

定理 2.1.1　集合 $A = B$ 等价于 $A \subset B$,同时 $B \subset A$。

定义 2.1.2　设集合 S 包含集合 A 与集合 B 中的所有元素,但不含其他元素,则称 S 为 A 与 B 的和集,记为

$$S = A \cup B$$

类似可定义有限个集合 $A_1, A_2, \cdots, A_n$ 的和集或无限个集合 $A_1, A_2, \cdots, A_n, \cdots$ 的和集。

为了简明起见,常用连并号 $\bigcup$ 来记有限的和或无限的和。例如

$$S = \bigcup_{k=1}^{n} A_k = A_1 \cup A_2 \cup \cdots \cup A_n$$

$$S = \bigcup_{k=1}^{\infty} A_k = A_1 \cup A_2 \cup \cdots \cup A_n \cup \cdots$$

连并号后面集合符号的脚标 k 称为哑指标,而连加号的上下标则表示哑指标的变化范围。

定义 2.1.3　设集合 P 包含集合 A 与集合 B 的所有共同元素但不含其他元素,则称 P 为 A 与 B 的交集,记为

$$P = AB \text{ 或 } P = A \cap B$$

类似可定义有限个集合 $A_1, A_2, \cdots, A_n$ 的交集或无限个集合 $A_1, A_2, \cdots, A_n \cdots$ 的交集。

为了简明起见,常用连乘号 $\prod$ 来记有限的交或无限的交。例如

$$P = \prod_{k=1}^{n} A_k = A_1 A_2 \cdots A_n = A_1 \cap A_2 \cap \cdots \cap A_n$$

$$P = \prod_{k=1}^{\infty} A_k = A_1 A_2 \cdots A_n \cdots = A_1 \cap A_2 \cap \cdots \cap A_n \cap \cdots$$

例 2.1.1　$\prod_{k=1}^{\infty}\left(-\frac{1}{k}, \frac{1}{k}\right) = \{0\}$(单元素集)。

例 2.1.2　$\prod_{k=1}^{\infty}\left(0, \frac{1}{k}\right) = 0$(空集$\varnothing$)。

如果集合 A 与 B 没有共同元素,则记为 $A \cap B = \varnothing$,这时也称 A 与 B 是不相交的。

集合的运算和普通算术的运算有很多相似之处,例如:

定理 2.1.2

(1) $A \cup B = B \cup A$;

　$A \cap B = B \cap A$;

(2)$A \cup (B \cup C) = (A \cup B) \cup C$;

$A \cap (B \cap C) = (A \cap B) \cap C$;

(3)$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$;

$A \cup (B \cap C) = (A \cup B) \cap (A \cap C)$。

证明　我们只证明(3)中的第一个式子,其余式子可类似证明。

设 $S = A \cap (B \cup C)$,$T = (A \cap B) \cup (A \cap C)$。

设 $x \in S$,则 $x \in A$ 并且 $x \in B \cup C$。后面的式子表明,$x \in B$ 或 $x \in C$,因而 $x \in A \cap B$ 或 $A \cap C$,从而 $x \in (A \cap B) \cup (A \cap C)$。这就说明 $S \subset T$。

反之,如果 $x \in T$,则 $x \in A \cap B$ 或 $A \cap C$,这就是说 $x \in A$ 并且 $x \in B$ 或 C。因此 $x \in B \cup C$。由 $x \in A$ 和 $x \in B \cup C$ 就得出 $x \in A \cap (B \cup C) = S$。这就说明 $T \subset S$。

由 $S \subset T$ 和 $T \subset S$ 即得 $S = T$。

类似地可证明

$$A(B_1 \cup B_2 \cup \cdots \cup B_n) = AB_1 \cup AB_2 \cup \cdots \cup AB_n$$

$$A(B_1 \cup B_2 \cup \cdots \cup B_n \cup \cdots) = AB_1 \cup AB_2 \cup \cdots \cup AB_n \cup \cdots$$

如果 $A \subset B$,则显然有

$$A \cup B = B,\text{特别 } A \cup A = A$$

$$A \cap B = A,\text{特别 } A \cap A = A$$

上面的例子说明,虽然集合的运算和普通算术的运算有很多相似之处,但它们又不完全相同。

定义 2.1.4　设 A,B 是两个集合,集合 R 包含属于 A 而不属于 B 的一切元素且除此之外不包含其他元素。则称 R 是 A 与 B 的差集,记为

$$R = A \setminus B$$

例如 $A = \{1,2,3,4\}$,$B = \{3,4,5,6\}$,则

$$A \setminus B = \{1,2\}$$

定义 2.1.5　设 A 表示一个集合,则称所有不属于 A 的元素组成的集合为 A 的补集或余集。记为 A' 或 A^c。

有时需在一个较大的集合 X 中考虑所有不属于 X 的子集 A 的元素的集合,这一集合称为 A 相对于 X 的补集或余集。

定理 2.1.3

(1)$A \setminus B = A \cap B'$;

(2)$A(B \setminus C) = AB \setminus AC$。

此定理可仿照定理 2.1.1 的证明方法证明。请读者自己练习一下。

定理 2.1.4　$(A \setminus B) \cup B = A$ 的充分必要条件是 $B \subset A$。

证明　若 $(A \setminus B) \cup B = A$,则显然 $B \subset A$;反之若 $B \subset A$,则 $(A \setminus B) \cup$

$B \subset A$,另一方面由差集与并集的定义知,恒成立 $A \subset (A \setminus B) \cup B$,故必有 $(A \setminus B) \cup B = A$。

定理 2.1.3 以及下面的定理说明引进了补集的概念之后,集合的一切运算都可以归结为交和并的运算,因此并、交、补三种运算是集合的基本运算。

德摩根(De Morgan, Augustus, 1806—1871),英国数学家,生于印度的马德拉斯管区的马都拉,卒于伦敦.

定理 2.1.5 (德摩根公式)

(1) $(A \cup B)' = A' \cap B'$;

(2) $(A \cap B)' = A' \cup B'$。

证明 我们只证(1),(2) 类似可证。

设 $x \in (A \cup B)'$,则 $x \notin A \cup B$,因此 $x \notin A$ 并且 $x \notin B$。换句话说 $x \in A'$ 并且 $x \in B'$。因此 $x \in A' \cap B'$。由 x 的任意性就得出 $(A \cup B)' \subset A' \cap B'$。

反过来,如果 $x \in A' \cap B'$,那么 $x \in A'$ 并且 $x \in B'$。因此 $x \notin A'$ 并且 $x \notin B'$,因而 $x \notin A \cup B$,或者 $x \in (A \cup B)'$,因此 $A' \cap B' \subset (A \cup B)'$。

由以上两方面的论述即得出所需要的等式。

习题 2.1

1. 证明:$AB \cup C = (A \cup C)(B \cup C)$。

2.2 有限集合的势

当我们考虑一个集合时,除了我们定义这个集合的那些性质,集合中的元素的其他性质就都不予考虑了。如果考虑各种集合的共同性质,那么恐怕就只剩下集合的大小这一个性质了。但是有人可能要问:集合有大小吗?回答是起码对于有限集合,是可以考虑它的大小的。直观上看起来,元素多的集合就要比元素少的集合大。这点在战争中特别明显,两军对战,在武器水平相当的情况下,兵力多的一方将占有明显的优势。所以交战之前,估计敌我双方兵力的对比,就成为指挥员定下决心的重要依据。

定义 2.2.1 设 A 是一个有限集合,那么 A 的元素的个数就称为此集合的势,记为

$$|A| \text{或} \overline{\overline{A}} \text{或} \# A$$

如果 A 和 B 是两个有限集合,自然会发生一个问题是:它们所含的元素的个数是否相同?或者说它们的势是否相等。首先想到的一个办法就是去数一下它们各有多少元素。不过当元素的数目很大时,数数也不是一件很轻松的事。但是不数也可以解决问题。比如一个老师领了一班学生到教室来,她还不知道教师中的座位够不够。这时她可以请学生自己去找座位,如果找不到,就先站在教

室里。等学生都找完座位后，如果有站着的人，她就知道座位不够，如果有座位空着，她就知道，座位多了，如果既没有站着的人，也没有空着的座位，她就知道学生和座位一样多。这种方法的实质是在学生的集合 A 和座位的集合 B 之间建立一种对应，或者更严格一点叫做映射。其实数数还是在建立映射，不过数数时我们是在一个有限集合和一个标准的有限集合 $\{1,2\cdots,n\}$ 之间建立映射而已。所以首先我们要弄清楚映射的含义。

定义 2.2.2　设 A,B 是两个集合。如果对于 A 中的每一个元素 $a\in A$，都有一个法则 f 使得 B 中有一个唯一的元素 b 与它对应，就称法则 f 建立了一个集合 A 到集合 B 的映射。这时 b 称为 a 在映射 f 下的像，a 称为 b 在映射 f 下的原像。记为

$$a\to b \text{ 或 } b=f(a)$$

映射这个概念是一个非常一般的概念，中学里学过的函数概念，大学里才学到的矩阵算子的概念都可以包括在这个概念里面。因为它几乎没有什么特殊要求，所以适用的范围非常广泛。这个概念中只有两个要求，就是 A 中每一个元素必须有一个像，而且像是唯一的。而这些要求好像是不能再少了。注意，在映射的定义中，对原像并没有什么要求，因此原像不一定是唯一的。比如在映射 $y=x^2$ 中，-1 和 1 的像就都是 1。另外还要注意，B 中有的元素不一定有原像。比如还是上面所说的映射，如果 B 中有负数，那么 B 中所有的负数就都没有原像，还要注意，没有原像的元素本身不可能是像，因此 B 中不一定所有的元素都是像。

用 $f(A)$ 表示集合 $\{f(x)\mid x\in A\}$，也就是 B 中所有的像所组成的集合，那么显然有 $f(A)\subset B$。

如果 $f(A)=B$，那么对于每一个 $b\in B$，就至少有一个 $a\in A$ 使得 $f(a)=b$。否则就至少有一个 $b\in B$，而不存在任何 $a\in A$ 使得 $f(a)=b$，因此 $f(A)$ 不可能等于 B，这就与 $f(A)=B$ 矛盾。这时称 f 为满射或映上的。如果 f 是映上的，则显然有 $|A|\geqslant|B|$。

如果对于 A 中任意两个不同的元素 a_1,a_2 都有 $f(a_1)\neq f(a_2)$，那么就称 f 是单射。也就是说，对于单射如果原像不同，那么映出的像也不同。由此可以得出有多少个原像，就有多少个像（如果 f 不是单射，那就不一定是这样，比如对于映射 $f=x^2$，除了 $x=0$ 之外，一般是两个原像对应于一个像，这时就不是有多少个原像就有多少个像了）。也就是说，B 中的元素个数比 A 中元素个数只多不少（因为 B 中还可能包括那些不是像的元素），或者说 B 中的元素个数至少与 A 中一样多。即对于单射成立 $|A|\leqslant|B|$。

定义 2.2.3　如果一个映射 f 既是单射又是映上的，那么就称 f 是一个一一对应或 1—1 对应。

如果 f 是一个 1—1 对应，那么根据映射的定义可知，对于 A 中的每一个元素 a，有 B 中的唯一元素 b 与之对应，反过来，由于 f 是映上的，所以对于 B 中的每一个元素 b，存在 A 中的元素 a 与之对应，而由于 f 又是单射，因此 A 中与 b 对应的元素 a 也是唯一的。这也可以作为 1—1 对应的另一个定义。

定义 2.2.4 设 A 与 B 是两个集合，法则 f 使 A 的任意元素 a 有 B 的唯一元素 b 和它对应，并且使 B 的任意元素 b 也有 A 的唯一元素和它对应，则称 f 是集合 A 与 B 之间的一一对应或 1—1 对应。

可以证明，这一定义与定义 2.2.3 是等价的，刚才我们已从定义 2.2.3 推出这一定义，读者可自己练习一下从这一定义得出定义 2.2.3。

如果 A，B 是 1—1 对应的有限集合，那么它们的元素个数必然相等。假设不然，不妨设 A 的元素个数较少，那么我们把 A 中的元素和 B 中与它对应的元素一对一对地逐次拿去（注意：由于 A，B 是 1—1 对应的，因此彼此对应的元素是唯一的，因而我们的拿法也是唯一的）。由于 A 是有限集合，并且元素个数较少，所以拿到最后，A 必然首先变为空集，而 B 中还有剩余的元素，这些元素不可能与 A 中任何元素对应，这就与 A，B 是 1—1 对应的假设相矛盾，同样，如果假设 B 中的元素较少，也要得出矛盾，因此我们得出

定理 2.2.1 设 A，B 是 1—1 对应的有限集合，则必有 $|A| = |B|$，记为

$$A \sim B$$

这个定理的逆定理也成立。

对于有限集合，还有一个和势有关的原理，就是所谓加法原理。形象地说，假如桌子的两个抽屉里都放着一些苹果，那么桌子里的苹果个数就等于两个抽屉里的苹果数目之和。这一原理是我们通过大量的事实与长期积累的经验认识到的一条客观规律，是我们生活在其中的外部客观世界的一种本性。它不需要证明。把这个原理用数学的语言写出来就是：

法则 2.2.1（加法原理） 设 S 是有限集合，$S = A \cup B$，而 $A \cap B = \varnothing$，那么

$$|S| = |A| + |B|$$

注意，要使上面的公式成立，必须 A 和 B 不相交，否则这一公式就不成立。例如设 $S = \{1,2,3,4,5,6\}$，$A = \{1,2,3,4\}$，$B = \{3,4,5,6\}$，那么 S 中有 6 个元素，A，B 中各有 4 个元素，显然 $6 \neq 4 + 4$。

加法原理还可以推广到有限个集合的情况，即：

法则 2.2.2（推广的加法原理） 设 S 是有限集合，$S = A_1 \cup A_2 \cup \cdots \cup A_n$，而 $A_1, A_2, \cdots, A_n$ 两两不相交，那么

$$|S| = |A_1| + |A_2| + \cdots + |A_n|$$

加法原理可以简单地概括为一句话，即对于有限集合，整体等于局部的和。

由加法原理立刻可以得出另一条原理,即所谓抽屉原理:

法则 2.2.3(抽屉原理) 设集合 S 是 n 个两两不相交的集合的并,而 $|S|>n$,那么这 n 个集合中必有一个集合至少包含两个元素。

上面提到,如果 S 的子集不是两两不相交的,那么加法原理就不成立。那么在 S 的子集是可以相交的情况下,有没有用 S 的子集的势去计算 S 的势的公式呢?回答是有的。要想知道这个公式的表达式,我们首先要看看,在 S 的子集可以相交的情况下,加法公式发生了什么变化。本来在加法公式中,S 的势就等于各个子集的势之和,当 S 的子集可以相交时,我们从法则 2.2.1 下面的例子中可以看出,子集的势之和要比 S 的势大,那么为什么会多出来一些数呢?我们从最简单的情况来看。

设 $S=A\cup B$,当 $A\cap B\neq\varnothing$ 时,由于 A 和 B 都包含 $A\cap B$,所以你在算 $|A|+|B|$ 时,就把 $|A\cap B|$ 多算了一遍(算了两遍),这样算出来的数当然就多了,为了得出正确的结果,我们必须从 $|A|+|B|$ 中减去一个 $|A\cap B|$ 才对,因此正确的公式应该是

$$|S|=|A|+|B|-|A\cap B|$$

(如果 A 和 B 是不相交的,那么 $|A\cap B|=0$,于是在上面的公式中,$|A\cap B|$ 这一项就不会出现,我们就又重新得到加法公式)。在我们提到的例子里,$|A\cap B|=2$,现在你再看看,是不是就对了?事实上,我们现在得到 $4+4-2$,恰好等于 S 的元素个数 6。

为了看出一般情况下的公式,我们再看看 S 有 3 个子集 A,B,C 时的情况。这时 A,B,C 不仅包含 $A\cap B,B\cap C,A\cap C$,而且还包含 $A\cap B\cap C$。我们在算 $|A|+|B|+|C|$ 时,把 $|A\cap B|,|B\cap C|,|A\cap C|$ 都多算了一遍,把 $|A\cap B\cap C|$ 多算了两遍。因此应该从 $|A|+|B|+|C|$ 中减去 $|A\cap B|$,$|B\cap C|$,$|A\cap C|$ 才对,但是因为 $A\cap B,B\cap C,A\cap C$ 中都包含着 $A\cap B\cap C$,所以我们又减多了(减了三遍),因此还要再加上一个 $|A\cap B\cap C|$ 才对。这样最后的公式就应该是

$$|S|=|A|+|B|+|C|-|A\cap B|-|B\cap C|-|A\cap C|+|A\cap B\cap C|$$

我们用一个例子来检验一下这个公式。设

$$S=\{1,2,3,4,5,6\},A=\{1,2,3,4\},B=\{2,3,4,5\},C=\{3,4,5,6\}$$

那么

$$|S|=6,\ |A|=|B|=|C|=4,\ |A\cap B|=|B\cap C|=3$$
$$|A\cap C|=2,\ |A\cap B\cap C|=2$$

而 $4+4+4-3-3-2+2=6$,恰好是 S 的元素个数。通过这个公式,我们还有理由猜到一般的公式应该是设 $S=A_1\cup A_2\cup\cdots\cup A_n$,则

$$|S| = \sum_{1\leq i\leq n}|A_i| - \sum_{1\leq i<j\leq n}|A_i\cap A_j| + \sum_{1\leq i<j<k\leq n}|A_i\cap A_j\cap A_k| + \cdots + (-1)^{n-1}|A_1\cap A_2\cap\cdots\cap A_n|$$

要证明这个一般的公式，再像刚才那样说恐怕就有些绕嘴，说不清楚了。但是不难想到可以用数学归纳法去证明。当 $n = 2,3$ 时，我们刚才已经验证了这个公式的正确性。现在假设这个公式对一切小于或等于 $n(n\geq 2)$ 的自然数都成立。又设

$$S_1 = A_1\cup A_2\cup\cdots\cup A_n\cup A_{n+1} = S\cup A_{n+1}$$

那么，根据 $n = 2$ 时的结果就有

$$\begin{aligned}|S_1| = |S| + |A_{n+1}| - |S\cap A_{n+1}| = &\sum_{1\leq i\leq n}|A_i| - \sum_{1\leq i<j\leq n}|A_i\cap A_j| + \\ &\sum_{1\leq i<j<k\leq n}|A_i\cap A_j\cap A_k| + \cdots + \\ &(-1)^{n-1}|A_1\cap A_2\cap\cdots\cap A_n| + |A_{n+1}| - \\ &|(A_1\cup A_2\cup\cdots\cup A_n)\cap A_{n+1}|\end{aligned}$$

而

$$\begin{aligned}&|(A_1\cup A_2\cup\cdots\cup A_n)\cap A_{n+1}| = \\ &|(A_1\cap A_{n+1})\cup(A_2\cap A_{n+1})\cup\cdots\cup(A_n\cap A_{n+1})| = \\ &\sum_{1\leq i\leq n}|A_i\cap A_{n+1}| - \sum_{1\leq i<j\leq n}|A_i\cap A_j\cap A_{n+1}| + \\ &\sum_{1\leq i<j<k\leq n}|A_i\cap A_j\cap A_k\cap A_{n+1}| - \cdots + \\ &(-1)^{n-1}|A_1\cap A_2\cap\cdots\cap A_n\cap A_{n+1}|\end{aligned}$$

把上面的式子代入 $|S_1|$ 中就得出

$$\begin{aligned}|S_1| = |A_1\cup A_2\cup\cdots\cup A_n\cup A_{n+1}| = &\sum_{1\leq i\leq n+1}|A_i| - \sum_{1\leq i<j\leq n+1}|A_i\cap A_j| + \\ &\sum_{1\leq i<j<k\leq n}|A_i\cap A_j\cap A_k| - \cdots + \\ &(-1)^{n}|A_1\cap A_2\cap\cdots\cap A_{n+1}|\end{aligned}$$

因此由数学归纳法我们就证明了：

定理 2.2.2(容斥原理)　设 $S = A_1\cup A_2\cup\cdots\cup A_n$，则

$$|S| = \sum_{1\leq i\leq n}|A_i| - \sum_{1\leq i<j\leq n}|A_i\cap A_j| + \sum_{1\leq i<j<k\leq n}|A_i\cap A_j\cap A_k| + \cdots + (-1)^{n-1}|A_1\cap A_2\cap\cdots\cap A_n|$$

定理 2.2.2 还有另一种表述方法，称为逐步淘汰原理，现介绍如下：

定理 2.2.3(逐步淘汰原理)　设 S 是一个有限集合，$A_1, A_2, \cdots, A_n$ 是 S 的子集，$\overline{A_i} = S - A_i$，那么

$$|\overline{A_1}\cap\overline{A_2}\cap\cdots\cap\overline{A_n}| = |S| - \sum_{1\le i<j\le n}|A_i\cap A_j| + \sum_{1\le i<j<k\le n}|A_i\cap A_j\cap A_k| + \cdots + (-1)^n|A_1\cap A_2\cap\cdots\cap A_n|$$

证明 由定理 2.1.5 知

$$\overline{A_1}\cap\overline{A_2}\cap\cdots\cap\overline{A_n} = \overline{A_1\cup A_2\cup\cdots\cup A_n}$$

因此 $A_1\cup A_2\cup\cdots\cup A_n$ 和$\overline{A_1}\cap\overline{A_2}\cap\cdots\cap\overline{A_n}$ 是不相交的集合，故由加法原理和容斥原理即得

$$\begin{aligned}|\overline{A_1}\cap\overline{A_2}\cap\cdots\cap\overline{A_n}| &= |S| - |A_1\cup A_2\cup\cdots\cup A_n| = \\ &|S| - (\sum_{1\le i\le n}|A_i| - \sum_{1\le i<j\le n}|A_i\cap A_j| + \\ &\sum_{1\le i<j<k\le n}|A_i\cap A_j\cap A_k| + \cdots + \\ &(-1)^{n-1}|A_1\cap A_2\cap\cdots\cap A_n|) = \\ &|S| - \sum_{1\le i\le n}|A_i| + \sum_{1\le i<j\le n}|A_i\cap A_j| - \\ &\sum_{1\le i<j<k\le n}|A_i\cap A_j\cap A_k| + \cdots + \\ &(-1)^{n-1}|A_1\cap A_2\cap\cdots\cap A_n|\end{aligned}$$

特别，当上述和式中的各项都相等时，上述公式就成为

$$|\overline{A_1}\cap\overline{A_2}\cap\cdots\cap\overline{A_n}| = |S| - \mathrm{C}_n^1|A_1| + \mathrm{C}_n^2|A_1\cap A_2| - \mathrm{C}_n^3|A_1\cap A_2\cap A_3| + \cdots + (-1)^n|A_1\cap A_2\cap\cdots\cap A_n|$$

逐步淘汰原理也可以表述成下述两种形式之一：

定理 2.2.4

(1) 设集合 S 中不具有性质 P_i 的元素组成的集合为 $A_i(i=1,2,\cdots,n)$，则具有性质 $P_1,P_2,\cdots,P_n$ 的元素的个数为

$$|S| - \sum_{1\le i\le n}|A_i| + \sum_{1\le i<j\le n}|A_i\cap A_j| - \sum_{1\le i<j<k\le n}|A_i\cap A_j\cap A_k| + \cdots + (-1)^n|A_1\cap A_2\cap\cdots\cap A_n|$$

(2) 设集合 S 中具有性质 P_i 的元素组成的集合为 $A_i(i=1,2,\cdots,n)$，则 S 中既无性质 P_1 又无性质 $P_2,\cdots$，又无性质 P_n 的元素的个数为

$$|S| - \sum_{1\le i\le n}|A_i| + \sum_{1\le i<j\le n}|A_i\cap A_j| - \sum_{1\le i<j<k\le n}|A_i\cap A_j\cap A_k| + \cdots + (-1)^n|A_1\cap A_2\cap\cdots\cap A_n|$$

应用容斥原理和逐步淘汰原理的区别在于前者是对 S 的子集进行分组，而后者是对 S 的子集的余集进行分组；而共同之处在于要求分成的子集，以及它们之中两个两个，三个三个，…，乃至 n 个之间的交集都很容易计数。

逐步淘汰原则中的公式又称为筛公式，因为它与数论中的筛法有关系。

例 2.2.1 由 n 个神经结组成了一个平面上的神经网络模型，其中每两个神经结之间都有直线的线路相连，当激活此神经网络模型时，每个神经结都会向距离它最近的神经结发射一个脉冲（如果距离它最近的神经结不止一个，那么它就任意向其中的一个神经结发射脉冲）。证明每次激活此神经网络模型时，任何一个神经结至多收到六个脉冲。并说明，可以发生一个神经结收到六个脉冲的情况。

证明 假设某一个神经结收到了七个脉冲，那么这个神经结与向它发射脉冲的七个神经结之间的线路就形成了七个角，如图 2.2.1 所示。由于这七个角之和为 360°，因此根据抽屉原理，它们其中必有一个要小于 60°。不妨设这个角为 $\angle A_5OA_6$，而由于 $\triangle A_5OA_6$ 的内角和为 180°，因此再次根据抽屉原理可知 $\angle OA_5A_6$ 和 $\angle OA_6A_5$ 之中又必有一个大于 60°（比如说是 $\angle OA_6A_5$）。

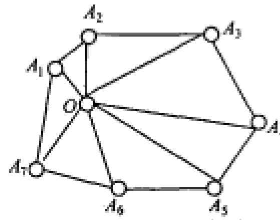


图 2.2.1

根据三角形中大角对大边的定理可知 $OA_5 > A_5A_6$。因此根据这个网络模型的特性，神经结 A_5 应该向神经结 A_6 发射脉冲，这与我们一开始所作的假设相矛盾。所得的矛盾说明神经结 O 不可能收到六个以上的脉冲。神经结 O 有可能收到六个脉冲。这只须有六个神经结与神经结 O 相连，且与神经结 O 相连的的六个神经结构成的多边形是一个正六边形，并且这六个神经结都向神经结 O 发射脉冲即可。

例 2.2.2 某班学生参加数、理、化三科考试，数、理、化优秀的学生分别为 30 人、28 人和 25 人；数理，理化，数化两科都优秀的学生分别为 20 人，16 人和 17 人；数理化三科全优的有 10 人。问数理两科至少有一科优秀的学生有多少人？数理化三科至少有一科优秀的学生有多少人？

解 用 A_1, A_2, A_3 分别表示数、理、化成绩优秀的学生组成的集合，那么根据容斥原理，数理两科至少有一科优秀的学生的数目为

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2| = 30 + 28 - 20 = 38$$

数理化三科至少有一科优秀的学生的数目为

$$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_2 \cap A_3| -$$

$$|A_1 \cap A_3|+|A_1 \cap A_2 \cap A_3| =$$
$$30+28+25-20-16-17+10=40$$

例 2.2.3 从自然数列 1,2,3,4,5,⋯ 中依次划去 3 的倍数和 4 的倍数，但保留 5 的倍数不划去。问剩下的数中第 1 995 个数是多少？

解 由于 3,4,5 的最小公倍数是 60，所以划数的规律每 60 个数就会重复一次。我们只要弄清从 1 到 60 这 60 个数划完了该剩下些什么数，就可以知道所有剩下的数的规律了。设 $I=\{1,2,3,\cdots,60\}$，I 中 3 的倍数的集合为 A_1，4 的倍数的集合为 A_2，5 的倍数的集合为 A_3。因为 5 的倍数要保留下来，所以不管怎么划，划来划去都是在 $\overline{A_3}$ 中划。而划去的数显然属于 A_1 或 A_2，因此在 $\overline{A_3}$ 中剩下的数都属于 $\overline{A_1}\cap\overline{A_2}\cap\overline{A_3}$，而 A_3 和 $\overline{A_1}\cap\overline{A_2}\cap\overline{A_3}$ 显然不相交。又

$$|A_1|=60/3=20,\ |A_2|=60/4=15,\ |A_3|=60/5=12$$
$$|A_1\cap A_2|=60/(3\times 4)=5,\ |A_2\cap A_3|=60/(4\times 5)=3$$
$$|A_1\cap A_3|=60/(3\times 5)=4$$
$$|A_1\cap A_2\cap A_3|=60/(3\times 4\times 5)=1$$

因此根据加法原理和逐步排斥原理就知道在 1 到 60 这 60 个数中剩下的数共有

$$\begin{aligned}&|A_3|+|\overline{A_1}\cap\overline{A_2}\cap\overline{A_3}|=\\&|A_3|+|I|-|A_1|-|A_2|-|A_3|+|A_1\cap A_2|+\\&|A_2\cap A_3|+|A_1\cap A_3|-|A_1\cap A_2\cap A_3|=\\&|I|-|A_1|-|A_2|+|A_1\cap A_2|+|A_2\cap A_3|+\\&|A_1\cap A_3|-|A_1\cap A_2\cap A_3|=\\&60-20-15+5+4+3-1=36\end{aligned}$$

其实具体对于这道题，以上的计算完全可以不进行，因为我们最后反正是要具体地确定对这 60 个数，划完后，剩下的是哪些数（而不是只知道剩下了多少数）。这样剩下了多少数，就作为一个副产品自然而然地得到了。但是当对更复杂的情况要求只求出剩下多少数时，上面的方法便有了一般性。

同样道理，以后每 60 个数中就剩下 36 个数。现在把整个自然数列排成一个每行 60 个数的 60 列的无限长方阵 A 如下：

$$\begin{bmatrix}1,2,3,4,5,6,7,8,9,10,\cdots,60\\61,62,63,64,65,66,67,68,69,70,\cdots,120\\\vdots\\60(m-1)+1,60(m-1)+2,\cdots,60(m-1)+10,\cdots,60(m-1)+60=60m\\\vdots\end{bmatrix}$$

由此看出，第 m 行中的数为

$$60(m-1)+1,60(m-1)+2,\cdots,60(m-1)+60=60m$$

并且划数的结果就是从长方阵 $\boldsymbol{A}$ 中划掉 24 列，我们把这个剩下的长方阵记为 $\boldsymbol{B}$。

假设剩下的数位于 $\boldsymbol{A}$ 的第 $i_1,i_2,\cdots,i_{36}$ 列，那么它们就构成了 $\boldsymbol{B}$ 的第 1，2，…，36 列。与 $\boldsymbol{A}$ 的构成规律类似，$\boldsymbol{B}$ 的第 m 行中的数为

$$36(m-1)+i_1,36(m-1)+i_2,\cdots,36(m-1)+i_{36}$$

设剩下的第 1 995 个数为 x。由于 $1\,995=55\times36+15$，因此我们知道，x 位于 $\boldsymbol{B}$ 的第 56 行第 15 列（也即 i_{15} 所在的列，由直接观察可得 $i_{15}=25$）。显然在这个方阵上添上被划掉的数，并不影响 x 在 $\boldsymbol{A}$ 中所在的行与列，即剩下的第 1 995 个数在原来的长方阵中仍位于第 56 行，第 15 列。因此按照我们刚才得出的公式即得

$$x=60(56-1)+i_{15}=60(56-1)+25=3\,325$$

例 2.2.4 设 $|A|=n$，B 是 A 的所有子集所组成的集合，求 $|B|=?$

解 B 中元素可以分成 $n+1$ 个互不相交的子集 $B_0,B_1,\cdots,B_n$，其中 B_0 是空集（A 的子集），B_1 是 A 中所有一个元素组成的 A 的子集所成的集合（这个集合构成 B 的一个子集），B_2 是 A 中所有两个元素组成的 A 的子集所成的集合，…，B_n 是 A 中所有 n 个元素组成的 A 的子集所成的集合。由组合知识可知：B_0 中含有一个集合（B 中的元素都是集合），B_1 中含有 C_n^1 个集合，B_2 中含有 C_n^2 个集合，…，B_n 中含有 C_n^n 个集合，因此

$$|B_n|=1+C_n^1+C_n^2+\cdots+C_n^n=(1+1)^n=2^n$$

习题 2.2

1. 证明：不可能存在对全体实数都有定义的函数 f，使得 $f(f(x))=x^2-2$。

2. 证明：不可能存在对全体实数都有定义的连续函数 f，使得 $f(f(x))=-x^3+x^2+1$。

3. (1) 设 f 是 $[0,+\infty)\to[0,+\infty)$ 的满足 $f(f(x))=3x$ 的严格单调递增的连续函数，举例说明，满足这些条件的连续函数不是唯一的；

(2) 设 f 是对所有自然数有定义并且取值也是自然数的严格单调递增的函数，满足函数关系 $f(f(n))=3n$。证明：满足这些条件的函数是唯一的，并求出 $f(1\,994)$ 的值。

4. 设有一座圆形的公园，中心为 O，半径等于 50 m。以点 O 为坐标原点，任取过 O 的互相垂直的两条直线为坐标轴，并设单位长为 1 m，这样就建立了一个坐标系。现在在园内除点 O 之外的每个整点处都种上一个小树。假设所有树干的横断面都是半径为 r 的圆。证明：当 $r>1/50$ 时，从点 O 朝任何方向看去，

视线都会被遮断；而当 $r < \frac{1}{\sqrt{2\,501}}$ 时，至少在一个方向上视线不会被遮断。

5. 将3行9列的方格矩形用黑白两种颜色染色，证明：无论如何染色，至少有两列的颜色是相同的。

6. 用黑白两种颜色将3行7列的棋盘上的方格染色，证明：不论如何染色，棋盘上总存在一个四个角上方格颜色相同的由方格组成的矩形，而对4行6列棋盘，则存在一种染法，使棋盘上不含有这种矩形。

7. 有一个生产天平上用的铁盘的车间，由于工艺上的原因，只能把盘子的质量的精度控制在0.1 g的水平上(即假如要求盘子的质量为 a g，则生产出的盘子的实际质量只能控制在 a 克到 $a \pm 0.1$ g之间)。现在需要质量相差不超过0.005 g的两只铁盘来装配一架天平，问最少要有多少盘子，才能从中挑选出符合要求的两只铁盘？

8. 把66个直径为 $\sqrt{2}$ 的圆任意放到一个边长为10的正方形内，求证：必有两个圆有公共点。

9. 在一个半径等于6的圆内任意地放进6个半径为1的小圆。证明：还可以在大圆内再放入另一个半径为1的小圆，使它和刚才放入的6个小圆不相交。

10. n 名选手参加单打淘汰比赛，需要打多少场后才能决出冠军？

11. 一条铁路线上共有 n 个客站，问需要印制多少种车票才能满足需要？

12. 设 $\{A_1, A_2, \cdots, A_s\}$ 是集 X 的 n 元子集的族。族中任意 $n+1$ 个集的交不空，证明：$A_1 \cap A_2 \cap \cdots \cap A_s \neq \varnothing$。

13. $A_1, A_2, \cdots, A_n$ 都是 r 元的集合。如果对自然数 k，这族集中每 k 个的并都是 X，而每 $k-1$ 个的并都是 X 的真子集。证明：$|X| \geqslant C_n^{k-1}$。等号成立时，必有 $r = C_{n-1}^{k-1}$。

14. 设 $A_1, A_2, \cdots, A_n, \cdots$ 是一些集合(有穷个或无穷个)。令

$$\underline{A} = \bigcup_{m=1}^{\infty}(\bigcap_{n=m}^{\infty} A_n), \overline{A} = \bigcap_{m=1}^{\infty}(\bigcap_{n=m}^{\infty} A_n)$$

证明：$\underline{A} \subseteq \overline{A}$ 并举一个 $\underline{A} \subset \overline{A}$ 的例子。

15. 有7只茶杯，一开始的时候，口全朝下。每一次操作可以任意翻转其中4只，问是否能经过有限次操作，使得这7只茶杯的口全都朝上？

16. 非负实数 $a_1, a_2, \cdots, a_{100}$ 满足条件

$$a_1 + a_2 + \cdots + a_{100} < 300$$
$$a_1^2 + a_2^2 + \cdots + a_{100}^2 > 10\,000$$

证明：在这100个数中一定存在3个脚标不同的数 $a_i, a_j, a_k (1 \leqslant i < j < k \leqslant 100)$ 使得

$$a_i + a_j + a_k > 100$$

2.3 无限集合的势

在 2.2 中我们定义了有限集合的势的概念，对于有限集合，这一概念就等同于这一集合中的元素的个数。我们当初定义这一概念的时候，目地之一就是可以比较两个有限集合中元素的个数谁多谁少。另一个目的就是利用势这一概念得出一些计算势的有用的公式。现在我们要问，对于无限集合，是否也能比较它们的元素的多少呢?从直观的角度看，两个无限集合有时明显地可以看出其中一个的元素要比另一个“多”。比如看全体正整数的集合 N 和全体正偶数的集合 M 这两个集合

$$N = \{1,2,3,4,\cdots\}, M = \{2,4,6,8,\cdots\}$$

显然，M 中的元素 N 中全有，而 N 中有无限多个元素 M 中却没有，因此如果认为 M 的元素要比 N 中的元素“多” 似乎没有错。在我们考察的这种情况下，N 称为 M 的真子集，以上的观点抽象出来就是认为一个集合的“势”(注意：目前我们还没有定义无限集合的势，因此这里的势只是我们的一种直观的还没有定义的潜在的概念) 要比它的真子集的势“大” 或“多”(什么叫“大”，什么叫“多”，目前也没有严格的定义)。但是按照这种思路，首先你就默认了无限集合的“势”像有限集合的势，也就是像数那样可以互相比较的，其次要比较两个无限集合的“势”，他们就必须有包含关系。如果它们谁也不包含谁，我们就不知道怎么办了。

在科学研究中，当我们遇到一种以前还未遇到过的情况时是需要非常小心的，而当一条路走不通时，我们需要仔细地考虑一下还有没有其他路可走。

在以上的讨论中，我们的第一个默认是不够小心的，因为“势” 的概念在无限的情况下很可能出现了和有限的情况本质上不同的新性质，其次我们的考虑遇到了不知道怎么办的情况，这就促使我们思考还有没有其他的思路。

为了找出新的思路，我们必须对于有限集合的势是什么意思重新做更深入的思考。现在我们重新再问：说一个集合的势是 3 是什么意思?这个意思其实是，我们把所有的有限集合进行分类，把所有有 3 个元素的集合分成一类，并用一个符号 3 来代表这一类集合的一种特性(这种特性叫做多少)。所以说“势” 的本质是先对集合做一种分类，然后把同类的集合给予一种符号来代表这一类集合的一种特性(对于有限集合，这种特性叫做多少)。那么我们又是怎样对集合进行分类的呢?在第二节我们已经看到，是用 1—1 对应的方法。也就是说，我们把所有能互相 1—1 对应的集合算做一类，并用一个符号来代表。这种方法也可以推广到无限集合。因为无限集合之间也可以存在 1—1 对应。

定义 2.3.1 若集合 A 与 B 之间存在一个 1—1 对应，则称 A 与 B 是“对等”的，并记为 $A \sim B$。

下面举几个对等集的例子。

例 2.3.1 设 A 与 B 是一个长方形的一对平行边上的点的集合(图 2.3.1)，则

$$A \sim B$$

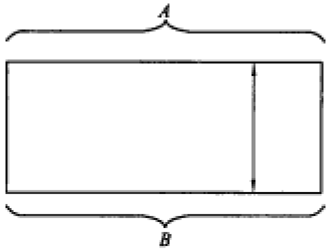


图 2.3.1

例 2.3.2 设 A 与 B 是两个同心圆圆周上的点的集合(图 2.3.2)。则显然

$$A \sim B$$

例 2.3.3 设 A 表示直角三角形斜边上的点的集合，B 表示底边上的点的(图 2.3.3)，那么由图 2.3.3 所示的 1—1 对应可以看出 $A \sim B$。

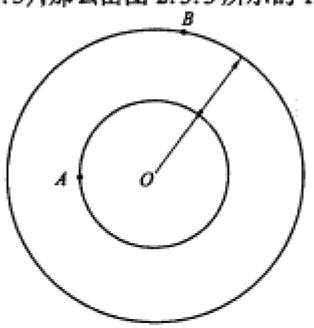


图 2.3.2

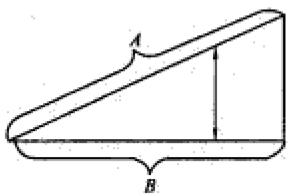


图 2.3.3

例 2.3.4 全体正整数的集合 $N = \{1,2,3,4,\cdots\}$ 和全体正偶数的集合 $M = \{2,4,6,8,\cdots\}$ 是对等的，这只要让 n 和 $2n$ 互相对应即可。

以下是几个关于对等集的简单性质。请读者自己证明作为练习。

定理 2.3.1

(1) $A \sim A$；

(2) 若 $A \sim B$，则 $B \sim A$；

(3) 若 $A \sim B, B \sim C$，则 $A \sim C$。

定理2.3.2 设 $A_1, A_2, \cdots$ 及 $B_1, B_2, \cdots$ 是两个集合的叙列，各集合 A_n 两两不相交，各集合 B_n 也两两不相交，且

$$A_n \sim B_n$$

则

$$\bigcup_{k=1}^{\infty} A_k \sim \bigcup_{k=1}^{\infty} B_k$$

有了对等的概念，我们就可把势的概念推广到无限集中了。

定义 2.3.2 所有对等的集合称为有相同的势，通常用一个符号来代表这个相同的势。

在上面的例子中，我们看出，在无限集中会出现一种有限集中没有的现象，即一个集合可能会和它的真子集对等(例如，例2.3.3中的 A 和 B，例2.3.4中的 M 和 N)。这是和我们的直观不一致的。但是为此而放弃对等的概念却是不值得的。对一些特殊的集合，我们也可以定义一些和直观相一致的反映集合中元素多少的概念，如长度、面积、体积等。但是这些概念只能适用于特殊的集合。比如长度，只适用于线段或与线段类似的曲线(这里又牵涉到什么是曲线的问题，这也不是一个简单的问题，本书中就不详细讨论这个问题了，有兴趣的读者可以参考这方面的专门著作) 这种集合，如果一个集合不是线段或曲线，长度这个概念就没有意义了。当然我们还可以把长度、面积、体积这些概念推广成一个叫测度的更广义的概念，用这个概念可以对更多的集合去度量它们中元素的多少。但是定义了测度这个概念后，又会发生一些奇怪的事情。例如会发生有的集合无法定义测度的问题，这也是和我们一开始的直观不一致的。所以世界上的有些事情就是这样，没有你所想象的那种十全十美的办法，遇到这种情况，我们只能放弃一些东西来得到一些东西。现在我们定义的势这个概念至少从三方面看是有点用处的。一是它对所有的集合都适用，不会发生对有的集合无法定义势的问题。因为所谓势就是对集合用对等的方法分类，并把所有属于一类的集合用一个符号代表就叫做这一类集合的势。如果一个集合不能和其他任何集合对等，那么它自己就构成一个类别，并会单独用一个符号来代表它，所以任何一个集合总是可以定义势这个概念的。第二，用对等这个概念可以得到一些新的东西，例如什么叫无限?你可以自己试试怎么说，似乎怎么说，绕来绕去，也只能在不是有限上打转转。以后可以看到用对等的概念就可以给无限一个严格的定义了。第三，我们还会看到，可以定义势的大小，这个概念很像整数之间的大小关系，因此也可以看成是整数的大小关系的一种推广(如果想到，整数其实不过是代表有限集合的势的符号，那么这一事实就显得应该是可以预料的)。

有限集中最简单的集合是空集或单元素集。它们的势分别是0或1，分别是非负整数和自然数中的最小数。那么无限集合中最简单的集合是什么呢?无限集合中最小的势又是什么呢?

定义 2.3.3 设 $M=\{1,2,3,\cdots\}$ 为全体正整数的集合，则称所有与集合 M 对等的集合 A 为可数集，或称 A 是可数的，并用 a 来代表可数集的势。

下面是几个可数集的例子：

$$A=\{1,4,9,16,\cdots,n^2,\cdots\}$$
$$B=\{1,8,27,64,\cdots,n^3,\cdots\}$$
$$C=\{1,\frac{1}{2},\frac{1}{3},\frac{1}{4},\cdots,\frac{1}{n},\cdots\}$$

显然，集合 A 是可数的充分必要条件是它可以写成 $A=\{a_1,a_2,a_3,\cdots,a_n,\cdots\}$ 的形式。

下面两个引理都是显然的：

引理 2.3.1 任何一个无限集合 A 必含有一个可数子集。

证明 这只要从 A 中每次取一个元素，由于 A 是无限集，因此这一过程可以无限进行下去，而我们因此就得到 A 的一个无限子集 B。按照从 A 中取出元素的先后顺序，A 必然可以写成 $A=\{a_1,a_2,a_3,\cdots,a_n,\cdots\}$ 的形式，所以 A 当然是一个可数集。

引理 2.3.2 可数集的任何无限子集仍是可数的。

证明 设 A 是可数集，B 是它的无限子集，将 A 写成

$$a_1,a_2,a_3,\cdots,a_n,\cdots$$

的形式，那么按照顺序一个一个看下去就会不断地遇到 B 的元素，而且 B 中的每个元素必定会被我们遇到，因此就有一个自然数与它对应。将 B 中的元素重新用从 1 开始的自然数编号，就可将 B 写成 $B=\{b_1,b_2,b_3,\cdots,b_n,\cdots\}$ 的形式，因此 B 是可数的。

以上两个引理从正反两方面说明可数集是最小的无限集。

引理 2.3.3 从可数集 A 中去掉一个有限子集 M 之后所得的 $A-M$ 仍为可数集。

证明 因为 $A-M$ 是 A 的无限子集，因此由定理 2.3.4 即知 $A-M$ 是一个可数集。

引理 2.3.4 设 A 是有限集，B 是可数集，则 $A\cup B$ 是可数集。

证明 不妨设 $A\cap B=\varnothing$，那么 $A\cup B$ 可表为 $\{a_1,a_2,a_3,\cdots,a_n,b_1,b_2,b_3,\cdots\}$ 形式，将 $A\cup B$ 重新编号即可知 $A\cup B$ 是可数的。如果 $A\cap B\neq\varnothing$，那么把 $A\cup B$ 分解成

$$(A\setminus A\cap B)\cup(A\cap B)\cup(B\setminus(A\cap B))=A\cup B$$

的形式，即可知 $A_1=(A\setminus A\cap B)\cup(A\cap B)$ 仍是有限集，$B_1=B\setminus(A\cap B)$ 仍是可数集(定理 2.3.5)，且 $A_1\cap B_1=\varnothing$，$A_1\cup B_1=A\cup B$，因此对 A_1,B_1 应用已证的结论就得到在这种情况下定理仍然成立。

以下几个定理中，我们都不妨设所需的集合是无公共元素的。

引理 2.3.5 有限个可数集的和集仍是一个可数集。

证明 我们只对三个可数集的情况加以证明，一般情形与此类似。设 A，B，C 是三个可数集，那么它们就可写成

$$A = \{a_1, a_2, a_3, \cdots\}$$
$$B = \{b_1, b_2, b_3, \cdots\}$$
$$C = \{c_1, c_2, c_3, \cdots\}$$

的形式，因此

$$A + B + C = \{a_1, b_1, c_1, a_2, b_2, c_2, a_3, b_3, c_3, \cdots\}$$

是可数的。

引理 2.3.6 可数个有限集的和集仍是可数集。

证明 设 $A_k(k = 1,2,3,\cdots)$ 是可数个有限集

$$A_1 = \{a_1^{(1)}, a_2^{(1)}, \cdots, a_{n_1}^{(1)}\}$$
$$A_2 = \{a_1^{(2)}, a_2^{(2)}, \cdots, a_{n_2}^{(2)}\}$$
$$A_3 = \{a_1^{(3)}, a_2^{(3)}, \cdots, a_{n_3}^{(3)}\}$$
$$\vdots$$

设 $S = \bigcup_{k=1}^{\infty} A_k$。我们先写出 A_1 中所有的元素，再写出 A_2 中所有的元素，依次类推，就可把 S 写成一个叙列，因此 S 也是一个可数集。

为了说话简明，我们引入下面的定义：

定义 2.3.4 说集合 A 是至多可数的意义为 A 是一个有限集或可数集。

用至多可数的术语可把引理 2.3.2 ~ 引理 2.3.5 合并成以下定理：

定理 2.3.3 可数集的子集是至多可数的。

定理 2.3.4 设 M 是可数集，A 是至多可数的，那么 $M + A$ 仍是一个可数集。

定理 2.3.5 可数个可数集的和集仍是一个可数集。

证明 设 $A_k(k = 1,2,3,\cdots)$ 是可数个可数集

$$A_1 = \{a_1^{(1)}, a_2^{(1)}, \cdots, a_3^{(1)}\cdots\}$$
$$A_2 = \{a_1^{(2)}, a_2^{(2)}, \cdots, a_3^{(2)}\cdots\}$$
$$A_3 = \{a_1^{(3)}, a_2^{(3)}, \cdots, a_3^{(3)}\cdots\}$$
$$\vdots$$

设 $S = \bigcup_{k=1}^{\infty} A_k$。我们先写 $a_1^{(1)}$（这时所有元素的上下标之和是2），然后再写第一列中的第二个元素 $a_1^{(2)}$，从 $a_1^{(2)}$ 沿从左下角到右上角的方向写下所有遇到的元素，即 $a_2^{(1)}$（这时所有元素的上下标之和是3），然后再回到第一列中的第三个

元素 $a_1^{(3)}$,从 $a_1^{(3)}$ 再沿从左下角到右上角的方向写下所有遇到的元素,即 $a_2^{(2)}$ 和 $a_3^{(1)}$(这时所有元素的上下标之和是 4)… 依次类推就可把 S 写成一个叙列,因此 S 也是一个可数集。

上面的这些定理也可以简明地用势的符号表示出来。设 n 和n_k 都表示有限集合的势(也就是它们都是自然数),a 代表可数集合的势,那么

$$a - n = a, a + n = a, a + a + \cdots + a = na = a$$

$$n_1 + n_2 + n_3 + \cdots = a, a + a + a + \cdots = aa = a$$

下面给出一个关于可数集的非常一般的定理:

定理 2.3.6 设 A 中的每一个元素都有有限个互相独立的下标,每一个下标可以是任意的自然数,则 A 是至多可数的集合。

证明 A 中每一个元素都可写成$a = a_{n_1, n_2, \cdots, n_k}$ 的形式,其中 $n_1, n_2, \cdots, n_k$ 都是自然数,k 也是自然数,依赖于 A 中的元素 a。我们令 a 与自然数

$$N(a) = 10^{n_1+n_2+\cdots+n_k} + 10^{n_2+\cdots+n_k} + \cdots + 10^{n_{k-1}+n_k} + 10^{n_k}$$

相对应。假设 A 中还有一个元素 $b = b_{m_1, m_2, \cdots, m_h}$,那么如果 $a \neq b$,那么它们所对应的数也必有 $N(a) \neq N(b)$。因为 N 写成十进位数之后就是一个由 0 或 1 组成的形如 10…010…010…010…0 的数,其中 1 的个数正好就是 k。所以如果 $N(a) = N(b)$,则 b 也必须有 k 个下标,即必有 $h = k$。由于 n_k 和 m_k 分别表示 a 和 b 所对应的数中从右往左数第一次出现 1 之前的 0 的个数。而 $N(a) = N(b)$,所以 $n_k = m_k$。同理 n_{k-1} 和 m_{k-1} 分别表示 a 和 b 对应的数中从右往左数在第一次出现 1 到第二次出现 1 之前的 0 的个数。因此 $n_{k-1} = m_{k-1}$,… 依次类推,我们最后得到 $n_1 = m_1$,这就得出 $a = b$。与一开始的假定矛盾。因此 A 中不同的元素必对应于不同的自然数。这就是说,A 对等于自然数集合的一个子集,因而是至多可数的(定理 2.3.3)。

注意:虽然上述定理中元素下标的个数 k 可以是任意的,而且对于不同的元素还可以不同,但是却必须每一次都是有限个下标,即不能用无限多个自然数($n_1, n_2, n_3, \cdots$) 来做一个元素的下标。(见定理 2.4.6 和第 6 章 6.4 中连分数的应用 I 定理 6.4.1)

下面讨论一般的无限集和可数集之间的关系。

引理 2.3.7 设 A 是至多可数的,M 是一个无限集,那么 M 和$M \cup A$ 的势相同,即 $M \cup A \sim M$。

证明 由定理 2.3.3 知 M 含有一个可数子集 D,设 $M - D = P$,则

$$M = P \cup D, M \cup A = P \cup (D \cup A)$$

由 $P \sim P, D \cup A \sim D$(定理 2.3.6 和定理 2.3.7) 即得 $M \cup A \sim M$。

上面所说的“设 A 是一个有限集或可数集” 这句话,以后也可简单地说成“设 A 是至多可数的”。

引理 2.3.8 如果 M 是一个不可数的无限集，A 是 M 的一个至多可数的子集，那么

$$M \setminus A \sim M$$

证明 差集 $B = M \setminus A$ 不可能是有限的，否则由 $M = A \cup B$ 得出 M 是至多可数的。这与我们对 M 所作的假定矛盾。因此 B 是一个无限集，由 $M = A \cup B$ 和定理 2.3.7 即得 $B \cup A \sim B$，而这就是 $M \setminus A \sim M$（$B \cup A = (M \setminus A) \cup A = M$）。

定理 2.3.7 任意无限集必含有一个和它自身对等的真子集。

证明 如果此无限集是可数的，那么从引理 2.3.3 得知它可与自身的一个真子集对等；而如果此无限集是不可数的，那么由引理 2.3.8 得知它可与自身的一个真子集对等。因此对任意的无限集，定理的结论都成立。

由此我们可以给予无限集一个正面的定义。

定义 2.3.5 可以和它的真子集 1—1 对应的集合称为无限集。

例 2.3.1 全体有理数所成的集合是可数的。

证明 所谓有理数就是可以表示成 $\frac{p}{q}$ 形状的数，其中 p 是整数，q 是非零的整数。

设 $\mathbf{Q}$ 是全体有理数所成的集合，$\mathbf{Q}^+$ 是全体正有理数，$\mathbf{Q}^-$ 是全体负有理数，那么

$$\mathbf{Q} = \mathbf{Q}^+ \cup \{0\} \cup \mathbf{Q}^-$$

$\mathbf{Q}^+$ 和 $\mathbf{Q}^-$ 显然是对等的。因此我们只要证明 $\mathbf{Q}^+$ 是可数的即可。首先写出分母是 1 的所有正有理数，显然这些有理数可以排成一个叙列，即

$$x_{11}, x_{12}, x_{13}, \cdots$$

其中 $x_{1n} = n/1$。然后再写出分母是 2 的所有正有理数，显然这些有理数也可以排成一个叙列，即

$$x_{21}, x_{22}, x_{23}, \cdots$$

其中 $x_{2n} = n/2$。然后再写出分母是 3 的所有正有理数，他们也可以排成一个叙列。依此类推，即可把所有的正有理数排成一个方阵如下

$$\begin{matrix} x_{11}, x_{12}, x_{13}, \cdots \\ x_{21}, x_{22}, x_{23}, \cdots \\ x_{31}, x_{32}, x_{33}, \cdots \\ \vdots \end{matrix}$$

然后仿照定理 2.3.5 的证明中所使用的方法，沿着一条由此方阵的各条从左下方到右上方的对角线所构成的蛇形曲线（即沿着 $x_{11} \to x_{21} \to x_{12} \to x_{13} \to x_{22} \to x_{31} \to x_{41} \to \cdots$ 所形成的路线）去看这个方阵中的有理数，看的时候把已

出现过的有理数都去掉，用这样的方法即可把全体正有理数写成一个叙列，因此就证明了 $\mathbf{Q}^+$ 是可数的，因而全体有理数也是可数的(引理 2.3.5)。

还可以用其他方法来证明全体有理数是可数的。比如对一个有理数 p/q，我们可定义一个称为“高度”的数如下：$h=|p|+|q|$。显然最小的高度是 1，对应的有理数只有一个，就是 0/1 或 - 0/1，同样显然的事情是高度一定的有理数是有限的，于是我们可以先写出所有高度等于 1 的有理数，然后再写出所有高度等于 2 的有理数，所有高度等于 3 的有理数等等。以下是一种写法 0/1，1/1，- 1/1，1/2，2/1，- 1/2，- 2/1，1/3，2/2，3/1，- 1/3，- 2/2，- 3/1，… 在这个序列中去掉已出现过的数就可把全体有理数写成一个叙列的形式，因而全体有理数是可数的。其实这只不过是引理 2.3.6 中所使用的方法的一个具体应用。

更不可思议的是一种比有理数多得多的数即所谓代数数的全体居然仍是可数的。

定义 2.3.6 如果一个数是一个整系数的多项式的根，则称这个数是一个代数数。

例 2.3.2 全体整系数多项式

$$a_0x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n$$

的集合是可数的。

证明 先固定 n，由定理 2.3.6 可知整系数的 n 次多项式的全体是可数的，再由定理 2.3.5 即得全体整系数多项式的集合是可数的。

例 2.3.3 全体代数数是可数的。

证明 由例2.3.2知全体整系数多项式的集合是可数的，又每个多项式只有有限个根，因此由引理 2.3.6 即得全体代数数是可数的。

由定理 2.3.6 还可得出以下结论：

例 2.3.4

(1) 平面上全体坐标为有理数的点(x,y)所成的集合是可数的；

(2) 所有形如$(n_1,n_2,\cdots,n_k)$(其中的 n_i 都是自然数) 的元素组成的集合是可数的。

2.4 不可数的集合

到现在为止，我们只知道一个无限的势即可数集合的势 a。于是自然产生一些问题：有没有不可数的势？是否有无限多的(无限的) 势？对这两个问题的回答都是肯定的。

首先说明，无限集不一定都是可数的。一个重要的例子如下：

定理 2.4.1 线段[0,1]中所有点的集合 U 是不可数的。

证明 假定 U 是可数的，那么 U 中所有的点就可以写成一个叙列

$$x_1, x_2, x_3, \cdots \tag{*}$$

用点$\frac{1}{3}$和点$\frac{2}{3}$把 U 分为三部分$[0,\frac{1}{3}]$，$[\frac{1}{3},\frac{2}{3}]$，$[\frac{2}{3},1]$，则其中必有一个不含有点 x_1（图 2.4.1）。用 U_1 表示这三部分中不含点 x_1 的线段（可能这三个线段中有两个都不含有 x_1，这时可取其中任意一个，例如左边的那一个）。

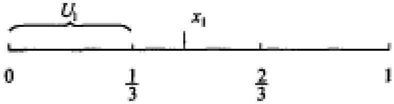


图 2.4.1

现在再将 U_1 分成三等份，取其中不含 x_2 的一个线段 U_2，然后再将 U_2 分成三等份，取其中不含 x_3 的一个线段 U_3，依次类推。

如此进行下去，我们就会得到一窜线段$\{U_i\}$，他们一个包含一个，形成一个区间套如下

$$U \supset U_1 \supset U_2 \supset U_3 \supset \cdots$$

且
$$x_n \notin U_n$$

注意线段 U_n 的长度是$\frac{1}{3^n}$，因此当 n 趋于无限大时，U_n 的长度趋于 0。从而必有一个点 ξ 适合

$$\xi \in U_n, n = 1,2,3,\cdots$$

（这是微积分中极限理论中的一条著名的定理，如果你现在还没有学微积分，那就不妨直观地想象一下，从直观上，这一结论也是很明显的）。

由于 ξ 是 U 中的一个点，因此根据我们的假定必有某一个自然数 n 存在，使得 $x_n = \xi$，但是根据 U_n 的构造过程又可知，无论 n 取什么值，总有

$$x_n \notin U_n, \xi \in U_n$$

从而得到
$$\xi \neq x_n$$

这显然是一个矛盾，所得的矛盾说明我们一开始所作的假定是错误的，因此 U 是不可数的。

根据上述事实，我们引入下面的定义：

定义 2.4.1 凡与区间[0,1]中所有的点对等的集合 A 都称为具有连续统的势，并用 c 来表示连续统的势。

定理 2.4.2 闭区间$[a,b]$，开区间(a,b)，半开区间$(a,b]$以及半开区间$[a,b)$的势都是 c。

证明 容易验证映射 $y = a + (b - a)x$ 是区间$[0,1]$和区间$[a,b]$之间

的 1—1 对应，因此区间$[a,b]$具有连续统的势。再由引理 2.3.8 可知，从区间$[a,b]$中去掉一个或两个点后所得的集合与区间$[a,b]$是对等的，因此开区间(a,b)，半开区间$(a,b]$以及半开区间$[a,b)$的势都是 c。

定理 2.4.3 有限个势为 c 的集合的并的势仍是 c。

证明 设 $S=\bigcup_{k=1}^{n}E_k$（由引理2.3.4下面的说明，我们不妨设 E_k 是两两不相交的），其中 E_k 的势都是 c。将半开区间$[0,1)$用 $n-1$ 个分点 $c_1,c_2,\cdots,c_{n-1}$ 分成 n 个半开区间如下

$$[0,c_1),[c_1,c_2),\cdots,[c_{n-2},c_{n-1}),[c_{n-1},1)$$

由于每一个半开区间的势都是 c，所以 E_1 和$[0,c_1)$，E_k 和$[c_{k-1},c_k)(k=2,3,\cdots,n-1)$，$E_n$ 和$[c_{n-1},1)$之间存在着1—1对应。把这些1—1对应合成起来就得到 S 和半开区间$[0,1)$之间的 1—1 对应。由于半开区间$[0,1)$的势是 c，因此 S 的势也是 c。

定理 2.4.4 可数个势为 c 的集合的并的势仍是 c。

证明 设 $S=\bigcup_{k=1}^{\infty}E_k$，其中每一个 E_k 的势都是 c。将半开区间$[0,1)$用可数个分点 $c_0=0<c_1<c_2<\cdots<c_{n-1}<\cdots$（其中 $c_k=\dfrac{k-1}{k}$，$k=1,2,\cdots$）分成可数个半开区间如下

$$[0,c_1),[c_1,c_2),\cdots,[c_{n-2},c_{n-1}),[c_{n-1},c_n),\cdots$$

由于每一个半开区间的势都是 c，所以 E_k 和$[c_{k-1},c_k)(k=2,3,\cdots,n,\cdots)$之间存在着1—1对应。把这些1—1对应合成起来就得到 S 和半开区间$[0,1)$之间的 1—1 对应。由于半开区间$[0,1)$的势是 c，因此 S 的势也是 c。

定理 2.4.5 全体实数的集合 Z 的势为 c。

证明 由于

$$Z=\bigcup_{k=1}^{\infty}\{[k-1,k)\cup[-k,-k+1)\}$$

故由定理 2.4.4 即得 Z 的势为 c。

定理2.4.6 设 $Q=\{(n_1,n_2,n_3,\cdots)\mid n_1,n_2,n_3,\cdots$ 都是自然数$\}$，则 Q 的势是 c。

证明 见第 6 章定理 6.4.1。

2.5 无限集的势的比较

现在我们已经知道了两个无限集合的势，即可数势 a 和连续统的势 c。我们知道，有限集合的势也就是自然数是可以互相比较大小的。既然无限集合的势

是有限集合的势的推广，那么无限集合的势是否能互相比较大小呢？回答是任何两个集合的势都是可以比较大小的，这又从另一个方面说明：无限集合的势的确是有限集合的势的推广。

那么怎样来比较两个无限集合的势的大小呢？我们仍然首先考察有限集合的势是如何比较大小的。说 $3>2$ 是什么意思呢？这首先表明一个势为 3 的集合和一个势为 2 的集合是不对等的，因为按照势的定义，凡是对等的集合就分成一类，并且用一个相同的符号来代表，这个符号就称为这一类集合的势。现在既然 3 和 2 是两个不同的符号，那么当然势为 3 的集合同势为 2 的集合是不可能对等的了。其次 $3>2$ 表明势为 3 的集合的一个子集是可以和势为 2 的集合对等的。这两条性质就可以推广到无限集合的势的比较上去。

定义 2.5.1 设集合 A 与 B 的势分别为 α 与 β，如果

(1) A 和 B 是不对等的；

(2) A 和 B 的一个子集对等。

则称 A 的势小于 B 的势，或说 B 的势大于 A 的势，记为 $\alpha<\beta$ 或 $\beta>\alpha$。

按此定义，我们就可知道 $1<2<3<\cdots<n<\cdots<a$。

又设

$$N=\{1,2,3,\cdots\},\overline{\overline{N}}=a$$
$$U=[0,1],\overline{\overline{U}}=c$$

由定理 2.4.1 知，N 和 U 是不对等的，但是 U 有一个子集 $U^*=\{1,\frac{1}{2},\frac{1}{3},\cdots\}$ 和 N 对等，因此由定义 2.5.1 可知 $a<c$。

那么有没有比 c 更大的势呢？回答是有。

定理 2.5.1 设 F 是所有定义在 $[0,1]$ 上的实函数的集合，则 F 的势大于 c。

证明 设 $U=[0,1]$。首先证明 F 与 U 不对等。假设不然，那么在 F 和 U 之间就存在着一种 1—1 对应：$t\to f_t(x)(0\leqslant x\leqslant 1)$，其中 $t\in U, f_t(x)\in F$。设

$$F(t,x)=f_t(x)$$

那么，$F(t,x)$ 是在 $0\leqslant t\leqslant 1, 0\leqslant x\leqslant 1$ 中定义的一个二元函数。

函数

$$\psi(x)=F(x,x)+1$$

显然是 F 中的元素，所以 U 中必有一个元素 a 使得 $f_a(x)=\psi(x)$，也就是 U 中必有一个元素 a 使得

$$F(a,x)=F(x,x)+1$$

现在取 $x=a$，得出 $F(a,a)=F(a,a)+1$，这显然是不可能的。所得的矛

盾说明 F 不可能与 U 对等。

但是 F 有一个子集 $F^{*} = \{\sin x + c\}(0 \leqslant c \leqslant 1)$ 和 U 对等($c \in U$ 与 $\sin x + c \in F^{*}$ 对应即可,则易于验证这个对应是一个 1—1 对应)。

这就证明了定理。

根据这个定理,我们引出以下定义:

定义 2.5.2 所有定义在[0,1] 上的实函数的集合 F 的势记为f。

由定理 2.5.1 知 $c < f$。

现在又要问,是否有大于 f 的势?回答仍然是肯定的。实际上,对于任何一个势,都存在比这个势更大的势。

定理 2.5.2 设 M 是一个集合,T 是 M 的一切子集组成的集合,那么

$$\overline{\overline{T}} > \overline{\overline{M}}$$

证明 因为 T 含有 M 的一切子集,所以 T 中包含 M 本身,空集,还包含 M 中每一个元素所成的单元素集。设 $T^{*} = \{\{m\} \mid m \in M\}$,则显然 $T^{*} \subset T$,T^{*} 和 M 对等。因此我们只须证明 T 和 M 不可能对等即可。

假设 T 和 M 是对等的,φ 是 T 和 M 之间的 1—1 对应。于是对于每一个 $m \in M$,T 中有一个唯一的 $\varphi(m)$ 和它对应,而 T 中每一个元素都一定可以写成 $\varphi(m)$ 的形式,其中 $m \in M$。

现在把 M 中元素分成两类:凡满足 $m \in \varphi(m)$ 的元素称为“好”的元素,否则称为“坏”的元素。这两类元素都不是空集,比如与 M 本身对应的元素便是好的,而与空集对应的元素便是坏的。于是 M 中的元素不是好的就是坏的。设 M 中所有坏元素的集合为 S,则 $S \in T$。而 M 中必有一个元素 m^{*} 使得

$$S = \varphi(m^{*})$$

现在我们提出一个问题:m^{*} 这个元素究竟是好的还是坏的呢?(注意 M 中的元素不是好的就是坏的) 我们会发现,无论怎么回答这个问题,都会得出矛盾。不信你看:如果说 m^{*} 是好的,那么按照好元素的定义便得出

$$m^{*} \in \varphi(m^{*}) = S$$

但是按照 S 的定义,是坏元素组成的集合,因此 $m^{*} \notin S$,我们得到一个矛盾;

那么如果设 m^{*} 是坏的呢?按照坏元素的定义便得出

$$m^{*} \notin \varphi(m^{*}) = S$$

这个式子表明,m^{*} 不是一个坏元素,这又是一个矛盾。由此得出 m^{*} 既非好的又非坏的。但是我们已经说过 M 中的元素不是好的就是坏的。于是无论怎样我们都会陷于矛盾,这一矛盾就说明 M 和 T 不可能对等。

由例 2.2.4 我们知道如果 M 是一个有限集,那么 $|T| = 2^{|M|}$。由此引出以下定义。

定义 2.5.3 若 M 的势为 μ，而 M 的所有子集组成的集合是 T，T 的势是 τ，则定义

$$\tau = 2^{\mu}$$

定理 2.5.2 表明

$$2^{\mu} > \mu$$

下面我们证明定理 2.5.3。

定理 2.5.3 $c = 2^{a}$。

证明 设 $\mathbf{N}$ 是自然数的全体，T 是 $\mathbf{N}$ 的所有子集的集合。按照符号的定义就有 T 的势是 2^{a}。设 $\mathbf{N}^{*} = (n_1, n_2, n_3, \cdots)$ 是 T 中的一个任意元素，令 $\mathbf{N}^{*}$ 对应于一个区间 $I = [0,1]$ 之间的二进小数 $a = 0.a_1a_2a_3\cdots$，对应的规则是：当 $i \in \mathbf{N}^{*}$ 时，令 $a_i = 1$，而当 $i \notin \mathbf{N}^{*}$ 时，令 $a_i = 0$。这些小数中有一部分从某一位起全是 1，设这种小数的全体是 S。那么 S 中的小数或者是 1 或者是 $\frac{m}{2^n}$，其中 $m < 2^n$，且 $m \neq 2^k$，$k = 1,2,3,\cdots n-1$。因此 S 是可数的。S 对应于 T 的一个子集 V。由于 S 是可数的，所以 V 也是可数的。于是 T/V 和 I/S 中的小数是 1—1 对应的（注意，如果不去除 S，则上述对应将不是 1—1 的。因为有可能有两个小数对应于同一个数。例如二进小数 0.1 和 0.0111111… 对应于同一个数 $\frac{1}{2}$。但是，只要排除了这种情况，上述对应就是 1—1 的了）。由引理 2.3.8 和定理 2.4.2 知 I/S，从而 T/V 的势是 c，再由引理 2.3.7 即知 T 的势也是 c。这就证明了定理。

根据定义 2.5.1，原则上两个集合的势就是可以比较的了。但是有的细心的读者可能还会提出一个问题，就是假如 A 有一个子集与 B 对等，B 又有一个子集与 A 对等时，该如何比较 A，B 的势呢？设 A，B 的势分别是 α 和 β，这从形式上就会得出 $\alpha \leqslant \beta$，同时又 $\alpha \geqslant \beta$，那到底 A 和 B 的势是什么关系呢？有的粗心的读者也去会说，那还不简单吗，应该是 $\alpha = \beta$。但是不要忘了，如果 α 和 β 是普通自然数，也就是有限集合的势，那么这是没有问题的，但是现在 α 和 β 代表任意集合包括无限集合的势，那就是一个需要重新研究的问题了。不过这样得出结论的读者还是值得鼓励的，虽然我们不能直接就认为 $\alpha = \beta$ 是一个不需要证明的结论，但是作为一个直观的猜想还有可能是合理的。在科学研究中，猜想虽然不能代替证明，但是一个合理的猜想往往也是很宝贵的线索，很多科学结果都是先有一个猜想，然后再获得严格证明的。

下面我们先证明一个引理，利用这个引理可以证明一个形式上类似于求极限方法中的"两边夹"定理。

引理 2.5.1 设 $A^{*} \subset A$，$B^{*} \subset B$，A 与 B 对等，A^{*} 与 B^{*} 对等，如果 A 与 B 之间的 1—1 映射法则和 A^{*} 与 B^{*} 之间的 1—1 映射法则相同，那么 $A \setminus A^{*}$ 与 $B \setminus B^{*}$ 就是对等的。

证明 设A与B之间的1—1映射法则是φ,那么φ只能把$A\setminus A^*$中的元素映到$B\setminus B^*$中去,否则将存在一个元素$a\in A\setminus A^*$,而$\varphi(a)\in B^*$,但是由于A^*与B^*是对等的,且A^*与B^*之间的1—1映射法则也是φ,因此又存在一个$a^*\in A^*$,而使得$\varphi(a^*)\in B^*$,显然$a\neq a^*$,这就与φ是1—1的性质矛盾,因此φ也是$A\setminus A^*$与$B\setminus B^*$之间的1—1映射。这就证明了引理。

注意在上面的引理中,如果去除"A与B之间的1—1映射法则和A^*与B^*之间的1—1映射法则相同"这一条件,那么这个引理一般来说是不成立的。最简单的例子可设A,B都是全体自然数的集合。$A^*=\{2,3,4,5\cdots\}$,$B^*=\{3,4,5,6,\cdots\}$。显然$A^*\subset A$,$B^*\subset B$。由于这四个集合都是可数的,因此它们之间是两两对等的。故条件"A与B对等,A^*与B^*对等"也是成立的,但是$A\setminus A^*=\{1\}$与$B\setminus B^*=\{1,2\}$显然是不对等的。

下面叙述并证明"两边夹"定理。

定理 2.5.4 设$A\supset A_1\supset A_2$,若$A\sim A_2$,则$A\sim A_1\sim A_2$。

证明 由于$A\sim A_2$,所以可设在A与A_2之间存在一个1—1对应φ,又由于$A\supset A_1\supset A_2$,所以又存在一个集合$A_3=\varphi(A_1)\subset A_2$(图2.5.1)。

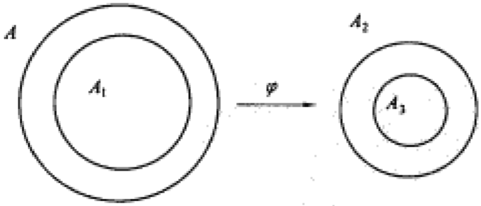


图2.5.1

由于$A_1\supset A_2\supset A_3$,$A_1\supset A_3$,$A_1$,$A_3$之间的1—1对应是$\varphi$,所以根据与上面同样的道理,又存在一个集合$A_4=\varphi(A_2)\subset A_3$。反复应用上面的论证就得到一串一个套一个的集合如下

$$A\supset A_1\supset A_2\supset A_3\supset A_4\supset\cdots\supset A_n\supset\cdots$$

使得$A\sim A_2$,$A_1\sim A_3$,$A_2\sim A_4$,$\cdots$,$A_n\sim A_{n+2}$,$\cdots$而且这些集合之间的对等都按照相同的法则对应。因此根据上面已证明过的引理2.5.1就有

$$\begin{aligned}A\setminus A_1&\sim A_2\setminus A_3\\A_1\setminus A_2&\sim A_3\setminus A_4\\A_2\setminus A_3&\sim A_4\setminus A_5\\&\vdots\end{aligned}\qquad(*)$$

又设$D=A\cap A_1\cap A_2\cap A_3\cdots$。现在你把这一串集合$A\supset A_1\supset A_2\supset A_3\supset A_4\supset\cdots\supset A_n\supset\cdots\supset D$想象成一串一个包含一个的同心圆,$D$就是这些

同心圆之中最里面的那个圆，而 $A \setminus A_1, A_1 \setminus A_2, A_2 \setminus A_3, \cdots$ 就是这些同心圆之间的圆环，显然这些圆环以及 D 是两两不相交的。而整个大圆就等于这些圆环叠加起来再叠加上 D(图 2.5.2)。因此我们可以把集合 A 和 A_1 用如下方式表示成一些两两不相交的集合的并

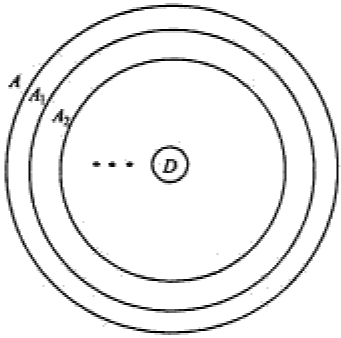


图 2.5.2

$$
\begin{aligned}
A = {} & (A \setminus A_1) + (A_1 \setminus A_2) + (A_2 \setminus A_3) + (A_3 \setminus A_4) + \cdots + = \\
& (A \setminus A_1) + (A_4 \setminus A_5) + (A_8 \setminus A_9) + (A_{12} \setminus A_{13}) + \cdots + \\
& (A_1 \setminus A_2) + (A_5 \setminus A_6) + (A_9 \setminus A_{10}) + (A_{13} \setminus A_{14}) + \cdots + \\
& (A_2 \setminus A_3) + (A_6 \setminus A_7) + (A_{10} \setminus A_{11}) + (A_{14} \setminus A_{15}) + \cdots + \\
& (A_3 \setminus A_4) + (A_7 \setminus A_8) + (A_{11} \setminus A_{12}) + (A_{15} \setminus A_{16}) + \cdots + D
\end{aligned}
$$

$$
\begin{aligned}
A_1 = {} & (A_1 \setminus A_2) + (A_2 \setminus A_3) + (A_3 \setminus A_4) + (A_4 \setminus A_5) + \cdots = \\
& (A_1 \setminus A_2) + (A_5 \setminus A_6) + (A_9 \setminus A_{10}) + (A_{13} \setminus A_{14}) + \cdots + \\
& (A_2 \setminus A_3) + (A_6 \setminus A_7) + (A_{10} \setminus A_{11}) + (A_{14} \setminus A_{15}) + \cdots + \\
& (A_3 \setminus A_4) + (A_7 \setminus A_8) + (A_{11} \setminus A_{12}) + (A_{15} \setminus A_{16}) + \cdots + \\
& (A_4 \setminus A_5) + (A_8 \setminus A_9) + (A_{12} \setminus A_{13}) + (A_{16} \setminus A_{17}) + \cdots + D
\end{aligned}
$$

由式(*)和上述 A 和 A_1 的表达式可以看出：

A 的第一行和 A_1 的第二行的各项是 1—1 对应的。

A 的第二行和 A_1 的第一行的各项是 1—1 对应的。

A 的第三行和 A_1 的第四行的各项是 1—1 对应的。

A 的第四行和 A_1 的第三行的各项是 1—1 对应的。

A 中的 D 和 A_1 中的 D 是 1—1 对应的。

这就证明了 A 和 A_1 是 1—1 对应的，因此 $A \sim A_1 \sim A_2$。

有了"两边夹"定理，就可以证明这一节最后的主要定理了。

伯恩斯坦(Бернштейн, Сергй Натанович, 1880—1968)，苏联数学家，生于敖德萨，卒于莫斯科.

定理 2.5.5(伯恩斯坦定理) 设 $A^* \subset A, B^* \subset B$, A 与 B^* 对等，B 与 A^*

对等,则 A 与 B 对等。

证明 由于 $B^{*}\subset B\sim A^{*}$,所以 A^{*} 必有一个子集 A^{**} 与 B^{*} 对等。而由定理的条件可知 $A^{**}\subset A^{*}\subset A$,又 $A\sim B^{*}\sim A^{**}$,故由已证的"两边夹"定理即得 $A\sim A^{*}\sim B$。

利用这个定理,我们就可以严格地证明上面提到的对无穷势的类似于有限势的性质的猜想了。

定理 2.5.6 设 α,β 是两个势,则下面三个关系式

$$\alpha<\beta,\alpha=\beta,\alpha>\beta$$

中的任何两个不可能同时成立。

证明 事实上,当关系式 $\alpha=\beta$ 成立时,按照符号的定义就可知其他两个当然都不会成立。

因此只须证明 $\alpha<\beta$ 与 $\alpha>\beta$ 不可能同时成立即可。假设不然,则可设集合 A 的势为 α,集合 B 的势为 β。按照 $\alpha<\beta$ 的定义有

(1) A 与 B 不对等;

(2) B 有一个子集 B^{*} 使得 $A\sim B^{*}$;

而按照 $\alpha>\beta$ 的定义,又有

(3) A 有一个子集 A^{*} 使得 $A^{*}\sim B$。

由(2),(3) 和伯恩斯坦定理即得 A 与 B 对等,而这与(1) 相矛盾。

定理 2.5.7 设 α,β,γ 是三个势,那么若 $\alpha<\beta,\beta<\gamma$,则 $\alpha<\gamma$。

证明 设集合 A,B,C 的势分别是 α,β,γ。则由 $\alpha<\beta,\beta<\gamma$ 的定义可知存在集合 B^{*} 和 C^{*} 使得 $A\sim B^{*}\subset B,B\sim C^{*}\subset C$,因此 C 中必存在一个集合 C^{**} 使得 $B^{*}\sim C^{**}$,因而有 $A\sim B^{*}\sim C^{**}\subset C$。我们证明 A 不可能与 C 对等。假设不然,则有 $B^{*}\subset B\subset C,A\sim B^{*}\sim C$,因此由"两边夹"定理即得 $B\sim C$ 或 $\beta=r$,而这与 $\beta<\gamma$ 矛盾。由 $A\sim B^{*}\sim C^{**}\subset C,A$ 与 C 不对等和 $\alpha<\gamma$ 的定义即得 $\alpha<\gamma$。这就证明了定理。

由势的大小的定义(定义 2.5.1) 即得:若 $A\sim B^{*}\subset B$,则或是 $\overline{\overline{A}}=\overline{\overline{B}}$,或是 $\overline{\overline{A}}<\overline{\overline{B}}$。如果把这句话简记为 $\overline{\overline{A}}\leqslant\overline{\overline{B}}$,那么定理2.5.7又可叙述成我们较为熟悉的形式如下。

定理 2.5.8 设 α,β 是两个势,那么如果 $\alpha\geqslant\beta$ 和 $\alpha\leqslant\beta$ 同时成立,则有 $\alpha=\beta$。

设 m 及 n 为两个自然数,则下面三个关系 $m<n,m=n,m>n$ 之中必成立一个且只成立一个。这称为自然数顺序的三歧性。那么对于无穷势,是否也有类似的性质呢?定理 2.5.7 已肯定这三个关系式只能成立一个。要证明无穷势也有类似于自然数顺序的三歧性。需要在一定的公理体系中讨论,这就牵涉到更基本的数学基础问题了。这已经超出了本书的讨论范围。

另外自然数还有一个重要的性质。就是存在一个最小的自然数，同时在连续两个自然数之间不存在任何其他自然数，对无穷势是否也可定义类似的概念呢？也就是是否也可把无穷势排成一个类似于自然数的顺序呢？更具体一些，我们要问在可数势 a 和连续统势 c 之间是否还存在着中间的势，这就是连续统假设。这是一个至今还没有解决的问题。

习题 2.5

1. 证明：平面上半径为有理数且圆心的坐标也为有理数的圆所组成的集合是可数的。

2. 证明：闭区间 $[a,b]$ 上的单调函数的间断点所组成的集合至多可数。

3. 证明：定义在整个数轴上的单调函数的间断点所组成的集合至多可数。

4. 证明：如果直线上的点集 E 的任何两点之间的距离大于 1，则 E 是至多可数的。

5. 已知平面点集 E 中任意两点之间的距离大于 a（$a>0$ 是一个正数），证明：E 至多可数。

6. 设 E 中的元素都是正数，且 E 是不可数的。证明：存在 $\tau>0$，使 $E\cap(\tau,+\infty)$ 不可数。

7. 下面这个命题是否成立？设 E 中的元素都是正数，且 E 是无限集，则存在 $\tau>0$，使 $E\cap(\tau,+\infty)$ 是无限集。证明你的结论或举出反例。

8. 设 E 是直线上的可数点集，是否可以将 E 移动一个距离 a（即将所有的点 $x\in E$ 换成 $x+a$），使得移动后所得的集合 E_a 不与 E 相交？

9. 设 E 是圆周上的可数点集，是否可以将圆周绕圆心旋转某一个角度 φ 使得 E 经旋转后所得的集合 E_φ 不与 E 相交？

10. 设 $f(x)$ 是定义在 $[0,1]$ 上的实值函数，且存在常数 M，使得对于 $[0,1]$ 中任意有限个数 $x_1,x_2,\cdots,x_n$ 均有 $|f(x_1)+f(x_2)+\cdots+f(x_n)|\leqslant M$。那么

$$E=\{x\in[0,1]\mid f(x)\neq 0\}$$

必是可数的。

11. 设 $f(x)$ 是定义在全数轴上的实值函数，如果对于任意的 x_0，必存在 $\delta>0$，使得当 $|x-x_0|<\delta$ 时，有 $f(x)\geqslant f(x_0)$，证明：函数 $f(x)$ 的所有函数值组成的集合是至多可数的。

12. 平面上两两不相交的 T 形字母（这些字母的大小可以不相同）组成的集合是否可以是不可数的？

13. 平面上两两不相交的 Γ 形字母（这些字母的大小可以不相同）组成的集合是否可以是不可数的？

14. 设 E 是定义在线段 $[a,b]$ 上的所有严格递增的连续函数组成的集合，

E 的势是什么?

15. 设 E 是定义在线段$[a,b]$上的所有单调函数组成的集合,E 的势是什么?

16. 证明:如果 $A \setminus B \sim B \setminus A$,则 $A \sim B$。

17. 证明:如果 $A \subset B$,且 $A \sim A \cup C$,则 $B \sim B \cup C$。

18. 设 E 是平面中的可数集,证明:存在互不相交的集合 A 和 B,使得 $E = A \cup B$ 且任一平行于 x 轴的直线与 A 至多交于有限个点,任一平行于 y 轴的直线与 B 至多交于有限个点。

19. 设 $E = A \cup B$,且 E 的势为 c,证明:A 和 B 中至少有一个集合的势也是 c。

20. 设 E 是直线上的点集,且 E 的势不大于 c,

$$A = \{(x_1, x_2, \cdots) \mid x_i \in E, i = 1,2,\cdots\}$$

证明:A 的势也不大于 c。

整数的性质

第三章

3.1 整数的顺序

整数是一种有着很好性质的整体，这首先表现在它是有顺序的。我们用 =，>，< 来描写数的顺序。关于这几个符号，我们规定：

法则 3.1.1

(1) $a = a$；

(2) $a = a$ 与 $a \neq a$ 不能同时成立；

(3) $a > b \Leftrightarrow b < a$；

(4) $a < b, b < c \Rightarrow a < c$。

整数是有顺序的，首先表现在任何两个整数之间是可以比大小的，其次在于这种比较大小的法则是随着整数的诞生自然产生的，在有了负数的概念之后，我们又把这种天然的顺序推广到负数之中，这就形成了以下的规定：

法则 3.1.2

(1) 在任何两个整数 a, b 之间，必定成立关系 $a > b, a = b, a < b$ 之中的一种，而且只成立一种；

(2) $0 < 1 < 2 < 3 < \cdots$；

(3) $a > b \Leftrightarrow a - b > 0$;

(4) $a + b$ 的符号与 a,b 中绝对值较大的数相同,其绝对值等于 a,b 中绝对值较大的数减去绝对值较小的数;

(5) ab 的绝对值等于 a 的绝对值乘以 b 的绝对值,当 a,b 的符号相同时,ab 的符号为正,当 a,b 的符号相反时,ab 的符号为负,0 和任何数的乘积仍为 0;

(6) $a < b, b < c \Rightarrow a < c$。

由以上几条法则就可以推出通常所说的不等式的以下几条性质:

法则 3.1.3

(1) 如果 $a > b$,那么 $a + c > b + c$;

(2) 如果 $a > b, c > 0$,那么 $ac > bc$;

如果 $a > b, c = 0$,那么 $ac = bc$;

如果 $a > b, c < 0$,那么 $ac < bc$;

(3) 如果 $a > b, c > d$,那么 $a + c > b + d$;

(4) 如果 a,b,c,d 都是正数,那么由 $a > b, c > d$ 得出 $ac > bd$;

(5) 如果 a,b 都是正数,n 是一个正整数,那么由 $a > b$ 得出 $a^n > b^n$。

整数除了是有顺序的,它还是离散的,也就是说,一个整数不管增大还是减小都至少要变化一个单位。这种性质反映在顺序关系中,就是以下法则。

法则 3.1.4 如果 $a < b$,那么 $a \leqslant b + 1$。

作为全体整数一部分的正整数也就是自然数,除了以上性质外,还具有一个称为良序性的性质(注意,这一性质不同于顺序性质,即有顺序性质的集合,不一定具有良序性)。可以证明,这一性质和数学归纳法是等价的,在本书中,我们可以把它视为不需证明的公理。

良序原理 设 T 是自然数的一个非空子集,那么 T 中必存在一个最小的自然数。

由良序原理立即得出:

推论 自然数的任何非空子集中不可能选取一个无穷的严格递减的序列。

良序原理保证了自然数非空子集中最小数的存在性,但是有时,这个最小数本身却不见得很小。例如可以证明方程

$$x^2 - 61y^2 = 1$$

存在无穷多组正整数解(即 x,y 都为正整数的解),因此根据良序原理,在这些解中,存在着一组解,使 x 最小,但是如果你想通过实验的方法找到这组解可不太容易。事实上,这组解的数值是 $x = 1\,766\,319\,049, y = 226\,153\,980$。再比如满足方程

$$x^2 + y^2 = z^2$$
$$x + y = w^2$$

的最小解是 $x = 4\ 565\ 486\ 027\ 761$，$y = 1\ 061\ 652\ 293\ 520$，$z = 4\ 687\ 298\ 610\ 289$。(这个方程的解在集合上的意义就是表示一个三条边都是整数的直角三角形的两条直角边之和也恰好是一个完全平方数)

习题 3.1

1. 设 $x_1, x_2, x_3, \cdots$ 是一个无界的由自然数组成的序列，则在此序列中可选出一个严格递增的子序列。

2. 设 $x_1, x_2, x_3, \cdots$ 是一个由自然数组成的序列，则在此序列中可选出一个不减的子序列。

3. 证明：对任意三个自然数的无限数列

$$a_1, a_2, \cdots, a_n, \cdots$$
$$b_1, b_2, \cdots, b_n, \cdots$$
$$c_1, c_2, \cdots, c_n, \cdots$$

总可选出脚标的严格递增的子序列 $n_1 < n_2 < n_3 < \cdots$ 使得

$$a_{n_1} \leqslant a_{n_2} \leqslant a_{n_3} \leqslant \cdots$$
$$b_{n_1} \leqslant b_{n_2} \leqslant b_{n_3} \leqslant \cdots$$
$$c_{n_1} \leqslant c_{n_2} \leqslant c_{n_3} \leqslant \cdots$$

4. 证明：从长、宽、高都是整数的长方体序列 $V_1, V_2, \cdots, V_n, \cdots$ 中必可选出一个无穷子序列，使得在此序列中的每一个长方体都可以套进后面一个长方体。

5. 设 M 是自然数的有上界的非空子集，则 M 中必存在一个最大数。

3.2　整数的整除性

整数是我们所使用的数字中最基本的数字，任何实际的计算最后都要归结为对整数的计算，因此，研究整数是研究任何一种数的基础。但是基础的东西就是刨根问底问到根上了，再没有任何更基础的东西去解释它。所以基础的东西往往更难，性质更复杂。

对两个整数可以实行加、减、乘、除四种运算，其中实行前三种运算的结果仍然得出整数。而实行除法所得的结果就不一定仍是一个整数了。所以除法在整数范围中具有特殊的地位，而整数的各种性质大都与除法有关。

用整数 b 去除整数 a，如果仍得出一个整数 c，我们就说 b 整除 a，并称 b 是 a 的因数，a 是 b 的倍数，设 c 是 a 除以 b 所得的商数，则

$$\frac{a}{b}=c$$

为简便起见，我们把上式记为 $b\mid a$，读作 b 整除 a。这时我们强调的是 a 除以 b 得出的商是一个整数，而在很多问题中，我们只要知道这一事实就够了，至于商的具体数值并不重要，这时采用上述记法就是非常方便的。整除的符号有以下性质：

定理 3.2.1

(1) $b\mid a\Leftrightarrow -b\mid a\Leftrightarrow b\mid -a$；

(2) $c\mid b,b\mid a\Rightarrow c\mid a$；

(3) $b\mid a,b\mid c\Rightarrow$ 对任意整数 m 和 n 有 $b\mid(ma+nc)$；

(4) $b\mid a,m\neq 0\Rightarrow mb\mid ma$；

(5) 设 $a\neq 0$，那么 $b\mid a\Rightarrow|b|\leqslant|a|$；

(6) $a\mid b$ 且 $b\mid a\Rightarrow|a|=|b|$。

这些性质都很容易证明，请读者自己验证。

当 $b\mid a$ 时，设 $a/b=c$，那么不难验证 $a/c=b$，也就是说，在 b 整除 a 时，因数和商是平等的，或商也是一个因数，因此不难设想，应该成立以下结果：

定理 3.2.2 设整数 $a\neq 0,d_1,d_2,\cdots,d_n$ 是它的全体约数。那么，$a/d_1,a/d_2,\cdots,a/d_n$ 也是它的全体约数，即当 d 遍历 a 的全体约数时，a/d 也遍历 a 的全体约数。特别，若 $a>0$，则当 d 遍历 a 的全体正约数时，a/d 也遍历 a 的全体正约数。

证明 当 $d\mid a$ 时，a/d 是一个整数。由于 $a=d(a/d)$，所以 a/d 也是 a 的约数。另外显然当 $d_1\neq d_2$ 时有 $a/d_1\neq a/d_2$。因此 $a/d_1,a/d_2,\cdots,a/d_n$ 是两两不同的，也就是说当 d 遍历 a 的全体约数时，a/d 就把 a 的约数两两不同地，因而又不多不少地重写了一遍，因此所有的 a/d 就只能还是 a 的全体约数。（注意：这里我们利用到了 a 的全体约数是有限的这一事实。如果 a 的全体约数不是有限的，就不能说明所有的 a/d 和 a 的全体约数这两个集合是同一个集合。例如当 n 遍历全体偶数时，$n+2$ 也是两两不同的偶数，但是 $n+2$ 并不遍历全体偶数）这就证明了定理的第一部分。注意到 a 的全体正约数也是有限的，就可类似地证明定理的第二部分。

例 3.2.1 证明：若 $3\mid n,7\mid n$，则 $21\mid n$。

证明 由 $3\mid n$ 知 $n=3m$，所以 $7\mid 3m$，由此及 $7\mid 7m$ 得出 $7\mid(7m-2\cdot 3m)=m$，故 $m=7k$，因此有 $n=3m=3\cdot 7k=21k$，这就证明了 $21\mid n$。

刚才我们讨论了整数 b 整除 a 的情况。但是当 a 除以 b 时，还可能发生另一

种情况，即 b 不能整除 a 的情况（记为 $b \nmid a$）。例如用 7 除以 3，除了得出商数是 2 以外，还会得出余数是 1。在小学里，我们把这一除法写成

$$7 \div 3 = 2 \cdots 1$$

但是这种写法既不方便又不能明显地表示出被除数，除数，商和余数这几个数之间的关系。事实上，上式中这几个数的关系是 $7 = 2 \cdot 3 + 1$；把这个例子推广到一般，就有：

定理 3.2.3（带余数除法定理） 若 a, b 是两个整数，$b > 0$，则存在唯一的两个整数 q 及 r，使得

$$a = bq + r, 0 \leqslant r < b$$

证明 考虑整数组成的序列

$$\cdots, -3b, -2b, -b, 0, b, 2b, 3b, \cdots$$

则 a 必在上述序列的某两项之间，即存在一个整数 q 使得

$$qb \leqslant a < (q+1)b$$

令 $a - qb = r$，则 $a = qb + r$，而且 $0 \leqslant r < b$。

现在证明上式中的 q 和 r 是唯一的。假设不然，则必存在着 q_1, r_1 及 q_2, r_2 使得 $q_1 \neq q_2$，并且

$$a = bq_1 + r_1$$

$$a = bq_2 + r_2$$

因而 $$bq_1 + r_1 = bq_2 + r_2$$

于是 $$b(q_1 - q_2) = r_1 - r_2$$

故 $$b \mid q_1 - q_2 \mid = \mid r_1 - r_2 \mid$$

由于 r_1 及 r_2 都是小于 b 的正数，所以上式右边是小于 b 的，而左边是大于等于 b 的。这是不可能的。因此必有 $q_1 = q_2$，因而 $r_1 = r_2$。

推论 $b \mid a$ 的充分必要条件是在 a 除以 b 的带余数除法公式中，余数 $r = 0$。

例 3.2.2 证明：$\underbrace{10\cdots01}_{200个0}$ 可被 1 001 整除。

证明 $$\underbrace{10\cdots01}_{200个0} = 10^{201} + 1 = (10^3)^{67} + 1$$

利用当 n 为一个正奇数时的因式分解公式

$$x^n + y^n = (x+y)(x^{n-1} - x^{n-2}y + \cdots - xy^{n-2} + y^{n-1})$$

即可得

$$(10^3)^{67} + 1 = (10^3 + 1)((10^3)^{66} - (10^3)^{65} + \cdots - 10^3 + 1)$$

而 $10^3 + 1$ 就是 1 001，所以 1 001 整除 $\underbrace{10\cdots01}_{200个0}$。

例 3.2.3 设 $m > n \geqslant 0$，证明：$(2^{2^n} + 1) \mid (2^{2^m} - 1)$。

证明 利用当 n 为一个正整数时的因式分解公式

$$x^n - y^n = (x - y)(x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1})$$

取 $x = 2^{2^n} + 1, y = 1$,并把 $k = 2^{m-n-1}$ 看成上述公式中的 n,即得

$$2^{2^m} - 1 = (2^{2^{n+1}})^{2^{m-n-1}} - 1 = (2^{2^{n+1}} - 1)(x^{k-1} + x^{k-2} + \cdots + x + 1)$$

因此 $$(2^{2^n} + 1) \mid (2^{2^m} - 1)$$

但是由平方差公式又有

$$2^{2^{n+1}} - 1 = (2^{2^n} + 1)(2^{2^n} - 1)$$

所以最后就得到

$$(2^{2^n} + 1) \mid (2^{2^{n+1}} - 1) \mid (2^{2^m} - 1)$$

例 3.2.4 设 $F_k = 2^{2^k} + 1, m > n$,则 $F_n \mid (F_m - 2)$。

这实际上就是例 3.2.3 的另一种写法。但是数学里经常会看到把同一个结论用另一种形式写出来就会在论证时起到很大的作用,所以不要认为这是没有什么意义的文字游戏。

习题 3.2

1.证明:若 $5 \mid n, 17 \mid n$,则 $85 \mid n$。

2.证明:若 $2 \mid n, 5 \mid n, 7 \mid n$,则 $70 \mid n$。

3.设 a, b 都是不等于零的整数,且存在两个整数 x, y 使得 $ax + by = 1$。证明:若 $a \mid n, b \mid n$,则 $ab \mid n$。

4.设 $ax + by = 1, a \mid bn$,则 $a \mid n$。

5.证明:$3 \mid n(n + 1)(2n + 1)$。

6.若 $ax_0 + by_0$ 是形如 $ax + by$(x, y 是任意整数,a, b 是两个不全为零的整数)的数中的最小正数,则$(ax_0 + by_0) \mid (ax + by)$,其中 x, y 是任意整数。

7.若 $x^2 + ax + b = 0$ 有整数根 $x_0 \neq 0$,则 $x_0 \mid b$。一般地,若 $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ 有整数根 $x_0 \neq 0$,则 $x_0 \mid a_0$。

8.判断以下方程有无整数根,若有则求出它们的所有整数根。

(1) $x^2 + x + 1 = 0$　　(2) $x^2 - 5x - 4 = 0$

(3) $x^4 + 6x^3 - 3x^2 + 7x - 6 = 0$　　(4) $x^3 - x^2 - 4x + 4 = 0$

9.某商店定制了两种盒子,其中一种能装 3 斤(1 斤 = 500 g)糖,另一种能装 6 斤糖。假定每个盒子都必须装满,请问能用这两种盒子来装完 100 斤糖吗?

10.证明:任意正整数 n 都可唯一地表示成 $n = 2^k h$ 的形式,其中 h 是奇数。

11.设 $n \geqslant 2, 1 = 2^{k_1}h_1, 2 = 2^{k_2}h_2, \cdots, n = 2^{k_n}h_n$,其中 $h_1, h_2, \cdots, h_n$ 都是奇数。

证明：存在唯一的 S 使得 $k_s = \max(k_1, k_2, \cdots, k_n)$。

12. 设 $n \geqslant 2$，k_s 的意义与 11 题中相同。$M = 2^{k_s-1}h_1h_2\cdots h_n$，$i = 1,2,\cdots,n$，则当 $i \neq s$ 时，$i \mid M$；当 $i = s$ 时，$i \nmid M$。

13. 证明：当 $n > 1$ 时，$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$ 不是整数。

14. 证明：当 $n > 1$ 时，$1 + \frac{1}{3} + \frac{1}{5} + \cdots + \frac{1}{2n-1}$ 不是整数。

3.3 最大公因数和最小公倍数

从因数这个概念出发就又可以引导出两个新的概念，即素数和公因数的概念。

任给一个整数 a，则 a 有两个显然的因数：1 和 a 本身。这两个因数称为一个整数的平凡因数。而 a 的其他因数，也就是使得 $1 < b < a$ 的因数 b（如果 a 有）则称为 a 的真因数。这样，就可以把全体整数分成三类：一类是除了 1 和它本身外没有其他因数的整数，这种数称为素数（在小学算术中称为质数），如 2，3，5，7 等等；另一类是除了 1 和它本身外还有其他真因数的整数，这种数称为合数，如 4，6，10，12 等等。第三类只包含一个数就是 1，它既不是素数也不是合数。

任给两个整数 a,b，如果整数 d 既是 a 的因数又是 b 的因数，则称 d 是 a,b 的公因数。显然，a,b 的公因数是有限的，因此以下定义是合理的：

定义 3.3.1 整数 a,b 的最大的公因数称为它们的最大公因数，记为 (a,b)。

类似，可定义多个整数 $a_1,a_2,\cdots,a_n$ 的最大公因数 $(a_1,a_2,\cdots,a_n)$ 的概念。

与最大公因数有关的另一个概念是所谓最小公倍数。任给两个整数 a,b，如果整数 1 既是 a 的倍数又是 b 的倍数，则称 1 是 a,b 的公倍数。显然 a,b 的正的公倍数有无穷多个，因此根据良序原理，下述定义是合理的：

定义 3.3.2 设整数 a,b 均不为零。那么它们的正的公倍数中的最小者称为它们的最小公倍数，记为 $[a,b]$。

类似，可定义多个整数 $a_1,a_2,\cdots,a_n$ 的最小公倍数 $[a_1,a_2,\cdots,a_n]$ 的概念。

下面我们首先来探讨一下这些符号本身的性质。首先可以看出，最大公因数和 a,b 二者的顺序没有关系，即显然有 $(a,b) = (b,a)$。其次，根据定理 3.2.1 中的结论(1)和最大公因数的定义可知最大公因数也和 a,b 二者的符号没有关系，即有 $(a,b) = (-a,b) = (a,-b)$。因此今后讨论两个数的最大公因数时，不妨设这两个数都是正数。第三，根据最大公因数的定义可知如果 a,b 二者之中有一个是 1，那么它们的最大公因数就是 1；如果 a,b 二者之中有一个

是另一个的倍数(不失一般性,不妨设 b 是 a 的倍数),那么 a,b 的最大公因数就是 a,特别,如果 a,b 二者之中有一个是 0,那么它们的最大公因数就是二者之中非零的整数。把这些内容写成定理就是:

定理 3.3.1

(1) $(a,b)=(b,a)$;

(2) $(a_1,a_2,\cdots,a_n)=(|a_1|,|a_2|,\cdots,|a_n|)$;

(3) 设 b 是任意非零整数,则 $(0,b)=|b|$。

其次,根据公因数的定义,我们可以证明以下的一个性质(学过行列式理论的读者可以看出它有点类似于行列式的一个性质)。

定理 3.3.2 设 q 是任意一个正数,则 $(a,b)=(a-bq,b)$。

证明 设 $c=a-bq$,d 是 a,b 的任一公因数,则由公因数的定义就有 $d\mid a,d\mid b$,因此由整数的整除性质(即 3.2 中定理 3.2.1(3))即知 $d\mid(a-bq)$,即 $d\mid c$,因此 d 是 b,c 的一个公因数,同理可证,b,c 的公因数必是 a,b 的公因数,由此显然就有 a,b 的最大公因数与 b,c 的最大公因数相同,这就证明了定理。这个证明实际上是先证明 a,b 的公因数集合与 b,c 的公因数集合相同,然后再得出它们的最大公因数相同,所以证明的过程与从定义证明两个集合相同的方法也是一样的。

虽然定理 3.3.2 的证明完全是从定义出发的很简单的证明,但是定理 3.3.2 却是一个很有用的定理。我们看以下的例子。

例 3.3.1 证明:对任意整数 n,$\dfrac{21n+4}{14n+3}$ 必是既约分数。

证明 只须证明这个分数的分子和分母的最大公约数必是 1 即可。由定理可得

$$\begin{aligned}(21n+4,14n+3)&=(21n+4-(14n+3),14n+3)=\\&(7n+1,14n+3)=(7n+1,14n+3-2(7n+1))=\\&(7n+1,1)=1\end{aligned}$$

以后演算熟了,就可直接写

$$(21n+4,14n+3)=(7n+1,14n+3)=(7n+1,1)=1$$

例 3.3.2 设 $F_k=2^{2^k}+1,k\geqslant 0$,证明:对于 $m\neq n$ 有 $(F_m,F_n)=1$。

证明 不妨设 $m>n\geqslant 0$,这里关键的一步是要看出 $F_n\mid(F_m-2)$(见3.2中例 3.2.4),故 $F_m-2=qF_n$,由此推出 $F_m=qF_n+2$,因此 $(F_m,F_n)=(qF_n+2,F_n)=(2,F_n)$,从而 $(F_m,F_n)\mid 2$,即 $(F_m,F_n)=1$ 或 $(F_m,F_n)=2$,但是 F_n 是一个奇数,因此 (F_m,F_n) 不可能等于 2,故必须 $(F_m,F_n)=1$。

例 3.3.3 证明:$(n!+1,(n+1)!+1)=1$。

证明 设 $d=(n!+1,(n+1)!+1)$,观察到等式 $(n!+1)(n+1)-((n+$

$1)!+1)=n$，则由 d 的定义即得 $d\mid n$，由此得 $d\mid n!$，再由 $d\mid(n!+1)$ 就得出 $d\mid(n!+1)-n!=1$，故 $d\mid 1,d=1$。

以上的几个例子的证明过程全都是简单的应用一下定理 3.3.2. 但是你如果光知道这个定理，恐怕不见得就能很顺利地解决这些问题，这里面每个问题中都有一个关键性的事实需要你知道或者观察出来。所以观察和发现问题中的一些数量关系、等式、性质等还是研究问题的一个基本功，需要自己长期积累。

从定理 3.3.2 出发，我们很容易地就可想到一个具体的求两个给定的正整数的最大公因数的方法。比如要求 (a,b) 是多少，不妨设 $a>b$。那么第一步就是从 a 中减去一个 b 的倍数，减去多少倍是随便的，只要使得剩下的数还是正的即可，但是为了使这个求最大公因数的过程快些，当然是要选的这个倍数在保持余数为正的前提下越大越好，那这其实就是用 b 去除 a 的算法，根据除法的法则这样剩下来的余数肯定比 b 小。因此第二步就是完全跟第一步相同的算法，只不过把两个数的位置换了，而因为我们已知道，最大公因数和两个数的位置是无关的，因此这是没有关系的。具体说第二步就是拿第一步得出的余数去除 b，然后反复进行这个算法，直到其中一个数是 0 或 1 为止，而因为每算一步，其中一个数，轮流地，都必定至少减少 1，因此算到最后，某个数必定是要变成 0 或 1 的。如果变成 0，则所求的最大公因数就是不为 0 的另一个数，如果变成 1，则这两个数的最大公因数就是 1。这么说很有点绕嘴，看几个具体例子就明白了。

例 3.3.4 求525 和 231 的最大公因数。

解 $(525,231)=(525-231\cdot 2,231)=(63,231)=(63,231-63\cdot 3)=$
$(63,42)=(63-42,42)=(21,42)=$
$(21,42-2\cdot 21)=(21,0)=21$

例 3.3.5 求169 和 121 的最大公因数。

解 $(169,121)=(169-121,121)=(48,121)=(48,121-48\cdot 2)=$
$(48,25)=(48-25,25)=(23,25)=(23,25-23)=$
$(23,2)=(23-2\cdot 11,2)=(1,2)=1$

如果到此为止，我们也就是找到了一种求两个数的最大公约数的算法而已，但是如果我们再进一步，把这个过程用公式写出来，那我们就可以得出更多的东西，这就是算术和代数的区别。其实现在我们所研究的问题跟我们在小学中学习除法时所遇到的问题没有什么本质的区别，区别就在于现在我们是用代数的方法去处理，结果就可得到许多新的很有用的结论。

把上面我们求两个数的最大公约数的算法用定理的形式写出来就是：

定理 3.3.3 设 a,b 是两个任意的正整数，由带余数除法，成立以下等式

$$a=bq_1+r_1,0<r_1<b$$

$$b = r_1 q_2 + r_2, 0 < r_2 < r_1$$
$$\vdots$$
$$r_{n-2} = r_{n-1} q_n + r_n, 0 < r_n < r_{n-1}$$
$$r_{n-1} = r_n q_{n+1}$$

那么,上述等式必只有有限步,并且$(a,b) = r_n$。

证明 因为每进行一次带余数除法,余数就至少减少1,而b是有限的,所以我们至多进行b次带余数除法,就可以得到一个余数是零的等式,即最后一个等式。由定理3.3.1和3.3.2即得

$$r_n = (0, r_n) = (r_n + 1, r_n) = (r_n, r_n - 1) = \cdots = (r_1, b) = (a, b)$$

这种算法,称为辗转相除法。在古代就已被中国的数学家发现,这就是中国古代的算学书中的求一术。但在外文书中,一般称这种算法为欧几里得算法。

欧几里得(Euclid,约公元前330—公元前275),希腊数学家.有关欧几里得的资料,多来自希腊学者普罗克洛斯.他认为,欧几里得生活的年代晚于柏拉图,早于阿基米得与埃及国王托勒密一世(Ptolemy I,约公元前306～公元前283)是同时代的人.

定理3.3.4 设(a,b)是两个任意的不全为零的整数,那么

(1) 若m是任意正整数,则$(am, bm) = m(a,b)$;

(2) 若δ是a,b的任一公因数,则$\left(\frac{a}{\delta}, \frac{b}{\delta}\right) = \frac{(a,b)}{|\delta|}$;

(3) $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1$。

证明 当a,b之中有一个为零时,定理显然成立。因此只须考虑a,b都不为零的情况即可。又由定理3.3.1可知不妨假定a,b都是正数。

(1) 在定理3.3.3中的各个等式的两边都乘以m即得

$$am = (bm)q_1 + r_1 m, 0 < r_1 m < bm$$
$$bm = (r_1 m)q_2 + r_2 m, 0 < r_2 m < r_1 m$$
$$\vdots$$
$$r_{n-2} m = (r_{n-1} m)q_n + r_n m, 0 < r_n m < r_{n-1} m$$
$$r_{n-1} m = (r_n m) q_{n+1}$$

再由定理3.3.3即得

$$(am, bm) = r_n m = (a,b)m$$

(2) 由(1)及定理3.3.1即得

$$\left(\frac{a}{\delta}, \frac{b}{\delta}\right)|\delta| = \left(\frac{|a|}{|\delta|}|\delta|, \frac{|b|}{|\delta|}|\delta|\right) = (|a|, |b|) = (a,b)$$

因此

$$\left(\frac{a}{\delta}, \frac{b}{\delta}\right) = \frac{(a,b)}{|\delta|}$$

(3) 在(2)中取$\delta = (a,b)$即得(3)。

定理3.3.5 a,b的公因数与(a,b)的因数相同。

证明 设$A = \{d \mid d 是 a,b 的公因数\}$,$B = \{d \mid d 是 (a,b) 的因数\}$。

如果 $d \in A$,那么由定理3.3.4(2)知 $|d|$ 是(a,b)的因数,从而 d 显然也是(a,b)的因数,故 $d \in B$,由此得出 $A \subset B$。反过来,如果 $d \in B$,那么 d 是(a,b)的因数,而由于(a,b)是 a,b 的最大公因数当然也是 a,b 的公因数,因此 d 显然也是 a,b 的因数,因而也是 a,b 的公因数,由此得出 $B \subset A$。由 $A \subset B$ 和 $B \subset A$ 即得出 $A = B$。

现在我们已经会求两个整数的最大公因数了,由此出发,即可求出多个整数的最大公因数。事实上,我们有下面的

定理 3.3.6 设 $a_1,a_2,\cdots,a_n$ 是 n 个整数,$d_2 = (a_1,a_2)$,$d_3 = (a_3,d_2)$,$\cdots$,$d_n = (a_n,d_{n-1})$,则

$$(a_1,a_2,\cdots,a_n) = d_n$$

证明 由定理的条件知 $d_n \mid a_n$,$d_n \mid d_{n-1}$。但是同样 $d_{n-1} \mid a_{n-1}$,$d_{n-1} \mid d_{n-2}$,故 $d_n \mid a_{n-1}$,$d_n \mid d_{n-2}$。依次类推可得 $d_n \mid a_n$,$d_n \mid a_{n-1}$,$\cdots$,$d_n \mid a_1$,这就说明 d_n 是 $a_1,a_2,\cdots,a_n$ 的一个公因数。反过来,设 d 是 $a_1,a_2,\cdots,a_n$ 的任一个公因数,则 $d \mid a_1$,$d \mid a_2$,故由定理3.3.5知 $d \mid d_2$,同样由定理3.3.5知 $d \mid d_3$,依次类推可得 $d \mid d_n$。因而 $d \leqslant |d| \leqslant d_n$,这就说明 d_n 是 $a_1,a_2,\cdots,a_n$ 的最大公因数。

下面再从辗转相除法得出一个很重要的但是却不是那么明显可以看出的定理。

定理 3.3.7 设 a,b 是两个任意的正整数,由带余数除法,成立以下等式

$$\begin{aligned}
a &= bq_1 + r_1, 0 < r_1 < b \\
a &= r_1q_2 + r_2, 0 < r_2 < r_1 \\
&\vdots \\
r_{n-2} &= r_{n-1}q_n + r_n, 0 < r_n < r_{n-1} \\
r_{n-1} &= r_nq_{n+1}
\end{aligned}$$

又设

$$\begin{aligned}
&P_0 = 1, P_1 = q_1, \cdots, P_k = q_kP_{k-1} + P_{k-2} \\
&Q_0 = 0, Q_0 = 1, \cdots, Q_k = q_kQ_{k-1} + Q_{k-2} \\
&k = 2,3,\cdots,n
\end{aligned}$$

那么(1) $$Q_ka - p_kb = (-1)^{k-1}r_k, k = 1,2,\cdots,n \qquad (*)$$

(2) 若 a,b 是两个不全为零的整数,则存在两个整数 λ,μ 使得

$$\lambda a + \mu b = (a,b)$$

(3) 两个整数 a,b 互素的充分必要条件是存在两个整数 λ,μ 使得

$$\lambda a + \mu b = 1$$

证明 (1) 当 $k = 1$ 时式$(*)$显然成立,当 $k = 2$ 时,由直接计算可得

$$Q_2a - P_2b = (q_2Q_1 + Q_0)a - (q_2P_1 + P_0)b = q_2a - (q_2q_1 + 1)b = q_2a - q_2q_1b - b = q_2(a - q_1b) - b = q_2r_1 - b = -r_2 = (-1)^{2-1}r_2$$

因此式(*)仍然成立。假定式(*)对不超过 $k \geqslant 2$ 的正整数都成立,则

$$Q_{k+1}a - P_{k+1}b = (q_{k+1}Q_k + Q_{k-1})a - (q_{k+1}P_k + P_{k-1})b = q_{k+1}(Q_ka - P_kb) + (Q_{k-1}a - P_{k-1}b) = (-1)^k(r_{k-1} - q_{k+1}r_k) = (-1)^kr_{k+1}$$

因此由数学归纳法就证明了对一切自然数 k,式(*)都成立。

(2) 由式(*)和定理 3.3.3 显然就得出定理 3.3.7 的第二部分。

(3) 如果 $(a,b) = 1$,那么由已证的结论(2)即知必存在两个整数 λ,μ 使得 $\lambda a + \mu b = 1$。反之,若存在两个整数 λ,μ 使得 $\lambda a + \mu b = 1$,则显然 $(a,b) \mid \lambda a + \mu b = 1$,故 $(a,b) = 1$。

定理 3.3.4 和 3.3.7 都可以很自然地从辗转相除法得出,其实,不使用辗转相除法也可以得出这两条定理,但你自己可以试一试,恐怕就没有这么省力,起码那个思路不是很明显的,需要你对最大公约数定义的本质有比较深的认识。所以辗转相除法不只是一个具体的算法,而且也是很有理论价值的。

定理 3.3.7 中最难的部分是(1),(1) 中的式(*),绝对不是一个容易自然发现的关系,所以它好像吸收了证明中的难点,也好像是在攻击的路线上先占领了一个制高点,以后从此制高点出发,再前进就容易了。下面我们就用定理 3.3.7 去证明一个很常用的数的整除性质。

定理 3.3.8 若 $(a,c) = 1, c \mid ab$,则 $c \mid b$。

证明 如果 $b = 0$,定理显然成立,因此可设 $b \neq 0$。

由 $(a,c) = 1$ 和定理 3.3.7 知存在两个整数 λ 和 μ 使得 $\lambda a + \mu c = 1$,又由 $c \mid ab$ 得 $ab = qc$,因此 $\lambda ab = \lambda qc$,而 $\lambda a = 1 - \mu c$,把此式代入前面的式子得 $(1 - \mu c)b = \lambda qc$,由此得出

$$b = \mu cb + \lambda qc = (\mu b + \lambda q)c$$

由于 $b \neq 0$,因此 $(\mu b + \lambda q) \neq 0$,这就得出 $c \mid b$。

定理 3.3.9 若 $(a,b) = 1, a \mid c, b \mid c$,则 $ab \mid c$。

证明 由 $a \mid c$ 得 $c = qa$, $b \mid qa$,再由 $(a,b) = 1$ 和定理 3.3.8 即得 $b \mid q$,因而 $ab \mid aq = c$。

定理 3.3.10 若 $(a,c) = 1$,则 $(ab,c) = (b,c)$。

证明 设 $A = \{d \mid d$ 是 ab 和 c 的公因数$\}$, $B = \{d \mid d$ 是 b 和 c 的公因数$\}$。

由 $(a,c) = 1$ 和定理 3.3.7 知存在两个整数 λ 和 μ 使得 $\lambda a + \mu c = 1$,用 b

去乘这个式子的两边，得 $\lambda ba + \mu bc = b$。

设 $d \in A$，则 $d \mid ab$，$d \mid c$，因此由上面的式子得出 $d \mid b$，这就说明 d 是 b，c 的公因数，即 $d \in B$，故 $A \subset B$。反过来设 $d \in B$，则 d 是 b，c 的公因数，因而显然也是 ab 和 c 的公因数，故 $d \in B$，因而 $B \subset A$。综合以上两方面的论述即得 $A = B$，由此即可推出

$$(ab, c) = (b, c)$$

定理 3.3.7(2) 可以推广到任意多个整数的情况，这就是下面的：

定理 3.3.11 设 $a_1, a_2, \cdots, a_n$ 是不全为零的整数，则

(1) $(a_1, a_2, \cdots, a_n) = \min\{s \mid s \in S\}$，其中 $x_i (i = 1, 2, \cdots, n)$ 都是整数；

$$S = \{s \mid s = x_1a_1 + x_2a_2 + \cdots + x_na_n, s > 0\}$$

(2) 存在一组整数 $\lambda_1, \lambda_2, \cdots, \lambda_n$ 使得 $(a_1, a_2, \cdots, a_n) = \lambda_1 a_1 + \lambda_2 a_2 + \cdots + \lambda_n a_n$。

证明 (1) 由于 $0 < a_1^2 + a_2^2 + \cdots + a_n^2 \in S$，所以 S 中存在着正整数元素，由最小数原理知 S 中必有一个最小的正整数，设这个最小的正整数为 s_0. 设 d 是 $a_1, a_2, \cdots, a_n$ 的任一个公约数，那么 $d \mid a_i$，$i = 1, 2, \cdots, n$，因此 $d \mid s_0$，故 $\mid d \mid \leqslant s_0$，另一方面，由带余数除法可得

$$a_i = q_is_0 + r_i, 0 \leqslant r_i < s_0, i = 1, 2, \cdots, n$$

由于 r_i 具有和 s_0 相同的形式（他们都是 $a_1, a_2, \cdots, a_n$ 的整数线性组合），所以对任意 i，r_i 必为零，否则就和 s_0 最小性相矛盾。这就说明 $s_0 \mid a_i$，$i = 1, 2, \cdots, n$。即 s_0 是 $a_1, a_2, \cdots, a_n$ 的公约数，由前半段的证明知 s_0 是最大的公约数，这就证明了(1) 的结论。

(2) 由(1) 已证和 s_0 定义知存在一组整数 $\lambda_1, \lambda_2, \cdots, \lambda_n$ 使得

$$s_0 = \lambda_1a_1 + \lambda_2a_2 + \cdots + \lambda_na_n$$

因此

$$(a_1, a_2, \cdots, a_n) = s_0 = \lambda_1a_1 + \lambda_2a_2 + \cdots + \lambda_na_n$$

下面我们开始讨论最小公倍数的性质。与定理 3.3.1 类似我们有以下的（请读者自己证明）

定理 3.3.12

(1) $[a, b] = [b, a]$；

(2) $[a_1, a_2, \cdots, a_n] = [\mid a_1 \mid, \mid a_2 \mid, \cdots, \mid a_n \mid]$。

因此以后讨论最小公倍数时只须考虑正整数即可。

定理 3.3.13 公倍数一定是最小公倍数的倍数。

证明 设 C 是 $a_1, a_2, \cdots, a_n$ 的公倍数，$L = [a_1, a_2, \cdots, a_n]$，则由带余数除法得

$$C = qL + r, 0 \leqslant r < L$$

从 c 和 L 都是 $a_1,a_2,\cdots,a_n$ 的公倍数和上式可知 r 也是 $a_1,a_2,\cdots,a_n$ 的公倍数。再由最小公倍数的定义和 $0\leqslant r<L$ 知 r 必为零，因此 $L\mid C$，这就证明了定理的结论。

和定理 3.3.4(1) 类似，对最小公倍数也有下面的

定理 3.3.14 设 $m>0$，则 $[ma_1,ma_2,\cdots,ma_n]=m[a_1,a_2,\cdots,a_n]$。

证明 设 $L=[ma_1,ma_2,\cdots,ma_n]$，$K=[a_1,a_2,\cdots,a_n]$。由 $ma_i\mid L$ 得出存在 q_i 使得

$$L=q_ima_i,i=1,2,\cdots,n$$

因此 $a_i\mid \frac{L}{m}$，$i=1,2,\cdots,n$，即 $\frac{L}{M}$ 是 $a_1,a_2,\cdots,a_n$ 的一个公倍数，因此由最小公倍数的定义即得 $K\leqslant\frac{L}{M}$。另一方面，由 $a_i\mid K$，得出 $ma_i\mid mK$，$i=1,2,\cdots,n$，即 mK 是 $ma_1,ma_2,\cdots,ma_n$ 的一个公倍数，因此由最小公倍数的定义即得 $L\leqslant mK$。结合上述两方面的论述即得 $L=mK$，这就是定理的结论。

定理 3.3.15 设 a,b 都是正整数，那么 $[a,b]=\frac{ab}{(a,b)}$，特别，如果 $(a,b)=1$，则 $[a,b]=ab$。

证明 设 $L=[a,b]$。首先考虑 $(a,b)=1$ 的情况，ab 显然是 a,b 的一个公倍数，因此由定理 3.3.13 知 $L\mid ab$。由 L 是 a,b 的公倍数得出 $a\mid L$，从而 $L=aq$，再由 $b\mid L=aq$，$(a,b)=1$ 和定理 3.3.8 得出 $b\mid q$，所以 $ab\mid aq=L$，$0<ab\leqslant L$，因此必有 $L=ab$，否则和 L 的最小性相矛盾。

对一般情形，即 (a,b) 不一定是 1 的情况，由定理 3.3.4 知

$$\left(\frac{a}{(a,b)},\frac{b}{(a,b)}\right)=1$$

因此对数 $\frac{a}{(a,b)},\frac{b}{(a,b)}$ 应用刚才已证明的结论即可得

$$\left[\frac{a}{(a,b)},\frac{b}{(a,b)}\right]=\frac{ab}{(a,b)^2}$$

再由定理 3.3.14 即得

$$[a,b]=\frac{ab}{(a,b)}$$

这就证明了定理。

与定理 3.3.6 类似，对最小公倍数也成立下面的

定理 3.3.16 设 $a_1,a_2,\cdots,a_n$ 是 n 个整数，$m_2=[a_1,a_2]$，$m_3=[a_3,m_2]$，$\cdots$，$m_n=[a_n,m_{n-1}]$，则

$$[a_1,a_2,\cdots,a_n]=d_n$$

证明 由 m_i，$i=2,3,\cdots,n$，的定义可知 $m_i\mid m_{i+1}$，$i=2,3,\cdots,n-1$ 以

及 $a_1 \mid m_2, a_i \mid m_i, i = 2,3,\cdots,n$。因此 m_n 是 $a_1,a_2,\cdots,a_n$ 的一个公倍数。又设 m 是 $a_1,a_2,\cdots,a_n$ 的任一个公倍数，则 $a_1 \mid m, a_2 \mid m$，故由定理 3.3.13 得 m 是 $[a_1,a_2]$ 的倍数，即 $m_2 \mid m$。同理，由 $m_2 \mid m$ 和 $a_3 \mid m$ 又得出 $m_3 \mid m$，依次类推，最后即得 $m_n \mid m$。因此 $m_n \leqslant |m|$，这就说明 m_n 是最小的公倍数，定理得证。

由于最大公约数可以实际地求出来，因此用定理 3.3.12 ~ 3.3.16 就可以实际的求出最小公倍数来。

例 3.3.6 从一张长2 002 mm，宽 847 mm 的长方形纸片上剪下一个边长尽可能长的正方形，如果剩下的部分不是正方形，那么在剩下的纸片上再剪一个边长尽可能长的正方形，按此方法不断重复，最后剪得的正方形的边长是多少毫米？

解 如图 3.3.1。

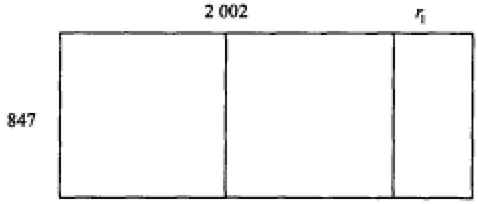


图 3.3.1

对 2 002 和 847 实行辗转相除法得到

$$2\,002 = 2 \times 847 + 308$$
$$847 = 2 \times 308 + 231$$
$$308 = 1 \times 231 + 77$$
$$231 = 3 \times 77$$

故最后剪下的正方形的边长为 77 mm。

例 3.3.7 设 $1\,993 \mid 11\cdots1$（共有 n 个 1），$A = (11\cdots1)(99\cdots9)(99\cdots9)\cdot(33\cdots3)$（每个数字都是 n 个）。证明：$1\,993 \mid A$。

证明 由等式 $A = 11\cdots1 \times (10\cdots090\cdots090\cdots030\cdots0)$（每个数字后面都是 n 个 0）即得。

如果你有计算机，并且在机器中安装了 MATLAB 软件，那么你就可以使用这个软件来帮你求出两个整数的最大公约数和最小公倍数来。求法如下。

打开 MATLAB 的命令窗口后，键入命令 gcd(x,y) 之后，按回车(Enter 键)，即可在屏幕中出现 x,y 的最大公约数。键入命令 lcm(x,y) 之后，按回车(Enter 键)，即可在屏幕中出现 x,y 的最小公倍数。这里 x 和 y 表示你想要输入的那两个整数。

习题 3.3

1. 把 19,20,…,77,80 连写成 $A = 1920\cdots7980$,证明:$1980 \mid A$。

2. 求 39 693 和 59 570 的最大公约数。

3. 狐狸和黄鼠狼进行跳跃比赛,狐狸每次跳 $4\frac{1}{2}$ m,黄鼠狼每次跳 $2\frac{3}{4}$ m。他们都每秒跳一次。在比赛途中从起点起,每隔 $12\frac{3}{8}$ m 设有一个陷阱,问当其中一个掉进陷阱时,另一个跳了多少米?

4. 一条公路由 A 经 B 到 C。已知 $AB = 280$ m,$BC = 315$ m,现在要在路边植树,要求树之间的间隔相等,且在 AB、BC 的中点都要种上树,那么两树间的距离最大能有多少米?

5. 设 $a_1, a_2, \cdots, a_n$ 及 b_1, b_2, b_m 是任意两组整数,且 $(a_i, b_j) = 1, i = 1, 2, \cdots, n, j = 1, 2, \cdots, m$,则

$$(a_1a_2\cdots a_n, b_1b_2\cdots b_m) = 1$$

6. 求满足 $(a,b) = 10, [a,b] = 100$ 的全部正整数组。

7. 求满足 $[a,b,c] = 10$ 的全部正整数组。

8. 求满足 $(a,b,c) = 10, [a,b,c] = 100$ 的全部正整数组。

9. 证明:若 $(a,4) = (b,4) = 2$,则 $(a+b,4) = 4$。

10. 设整数 a,b,c,d 满足 $ad - bc = \pm 1, u = ma + nb, v = mc + nd$,则 $(u,v) = (m,n)$。

11. 设 $a > b > 0, n > 1$,证明:$a^n - b^n$ 不可能整除 $a^n + b^n$。

12. (1) 设 $m = 2^n - 1, n \mid 2^n - 2$,则 $m \mid 2^m - 2$。

(2) 证明:$161\,038 \mid 2^{161\,038} - 2$。

13. 证明:存在无穷多个 n,使得 $n \mid 2^n + 1$。

14. (1) 设 $m = 2^n + 2, n \mid 2^n + 2, (n-1) \mid 2^n + 1$,则 $m \mid 2^m + 2, (m-1) \mid 2^m + 1$。

(2) 存在无穷多个 n,使得 $n \mid 2^n + 2$。

15. 证明:对任意正整数 a,存在无穷多个合数 n,使得 $n \mid a^{n-1} - a$。

16. 设 m,n 是正整数,证明:$(2^m - 1, 2^n - 1) = 2^{(m,n)} - 1$。

17. 设 $a > b, (a,b) = 1$,证明:$(a^m - b^m, a^n - b^n) = a^{(m,n)} - b^{(m,n)}$。

18. 设 a,m 是两个正整数,$(a,m) = 1$,k 是使得 m 能够整除 $a^k - 1$ 的最小正整数,又已知 m 能够整除 $a^n - 1$,证明必有 $k \mid n$。

3.4 素数和算数基本定理

在 3.3 中我们已经指出，从因数这个概念，就必然会从全体整数中分出一类称为素数的整数，现在我们确切地给出素数的定义。

定义 3.4.1 一个大于 1 的整数，如果它的正因数只有 1 和它本身，就称为素数或质数，否则就称为合数。

首先证明每一个大于 1 的整数必有质因数。

定理 3.4.1 设 a 是任意一个大于 1 的整数，则 n 的除 1 之外的最小的正因数 q 必定是一个素数，并且当 a 是合数时，$q \leqslant \sqrt{a}$。

证明 如果 q 不是素数，那么从素数的定义知，q 除了 1 和本身外还有一个正因数 q_1。显然 $1 < q_1 < q$。但是由于 $q_1 q, q \mid a$，所以 $q_1 \mid a$，这与 q 是 a 的除 1 之外的最小的正因数的条件相矛盾，因此 q 必定是一个素数。

当 a 是合数时，$a = pq$，且 $p > 1$，否则 a 将是一个素数。由于 q 是 a 的除 1 之外的最小的正因数，所以 $q \leqslant p, q^2 \leqslant pq = a$，因此 $q \leqslant \sqrt{a}$。

定理 3.4.2 设 p 是一个素数，a 是任意一个整数，则或者 a 与 p 互素，或者 p 整除 a。

证明 因为 $(p, a) > 0$ 是 p 的因数，而 p 只有两个正因数 1 或者 p。因此或者 $(p, a) = 1$，或者 $(p, a) = p$，即或者 $(p, a) = 1$，或者 $p \mid a$。

定理 3.4.3 设 $a_1, a_2, \cdots, a_n$ 是 n 个整数，p 是一个素数。如果 $p \mid a_1 a_2 \cdots a_n$，则 p 必定整除某一个 a_k。

证明 假定 $a_1, a_2, \cdots, a_n$ 都不能被 p 整除，则由定理 3.4.2 可知对 $k = 1, 2, \cdots, n$ 都成立 $(p, a_k) = 1$。因此由 $p \mid a_1 a_2 \cdots a_n$ 和 $(p, a_n) = 1$ 得出 $p \mid a_1 a_2 \cdots a_{n-1}$（定理 3.3.8），再由 $p \mid a_1 a_2 \cdots a_{n-1}$ 和 (p, a_{n-1}) 又得出 $p \mid a_1 a_2 \cdots a_{n-2}, \cdots$，依次类推，最后得出 $p \mid a_1$，而这与 $(p, a_1) = 1$ 矛盾，这就证明了定理。

下面我们证明整数的一个基本性质，就是所谓算术基本定理。

定理 3.4.4 任一大于 1 整数 a 必可唯一表示成

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}, \alpha_i > 0, i = 1, 2, \cdots, n$$

的形式，其中当 $i < j$ 时，$p_i < p_j$。

证明 由定理 3.4.1 知 a 的大于 1 的最小因数必定是一个素数 p_1，有素数的定义可知 $p_1 > 1$，因此 $a = p_1 a_1, a_1 < a$，同理 a_1 的大于 1 的最小因数必定是一个素数 p_2，故 $a_1 = p_2 a_2, a = p_1 p_2 a_2, a_2 < a_1 < a, \cdots$ 依次类推，由于 a 是一个有限数，数列 $a, a_1, a_2, \cdots$ 是严格递减的，因此最后必存在某一个自然数 m

使得 $a_{m+1} = 1$，这样，我们就可把任一个整数 a 分解成一窜素数的乘积 $a = p_1p_2\cdots p_m$ 经过重排次序，就可得到 $p_1 \leqslant p_2 \leqslant \cdots \leqslant p_m$。下面只须证明这种分解式是唯一的即可。

假设 a 还有另一种分解式 $a = q_1q_2\cdots q_k$，其中 $q_1, q_2, \cdots, q_k$ 都是素数，且 $q_1 \leqslant q_2 \leqslant \cdots \leqslant q_k$。那么显然有 $p_1p_2\cdots p_m = q_1q_2\cdots q_k$. 由定理 3.3.8 必存在两个数 p_i, q_j 使得 $p_1 \mid q_j, q_1 \mid p_i$。但是由于 p_1, q_1, p_i, q_j 都是素数，故必有 $p_1 = q_j$，$q_1 = p_i$。又 $p_i \geqslant p_1, q_j \geqslant q_1$，故 $q_j = p_1 \leqslant p_i = q_1$，因而 $p_1 = q_j = q_1$。把此式代入上面的两种分解式，便得 $p_2\cdots p_m = q_2\cdots q_k$，同理可得 $p_2 = q_2$。依次类推，最后即得 $m = k, p_i = q_i, i = 1,2,\cdots,m$。

最后再把所得的唯一的分解式中相同的素数合并在一起写成指数形式，并重新编号，就证明了定理。

有了这个定理，一个合数 a 的所有的因子的结构也就清楚了，这就是 a 的任一个因子 b 与 a 具有形同的形式，所不同的就是：在 b 的表示式中，有的指数可以为零，同时不能超过 a 的分解式中各个素数的指数。

虽然有了这个定理，我们对一个整数的因子的结构就清楚了，但是实际求出一个整数的所有素因数仍是一个极为困难的任务。借助于计算机和 MATLAB 软件，我们可以很轻松地完成这一任务。求法是：打开 MATLAB 的命令窗口，命令窗口中键入命令 factor(n) 之后，按回车(Enter) 键，即可在屏幕上出现整数 n 的素因子分解。使用这一命令时要求所输入的数字小于 2^{32} 如果你想对大于 2^{32} 的整数分解素因数，那么必须结合符号运算，具体命令如下：

factor(sym('n'))

或者先键入　　　　　　　　A = sym('n')

然后回车，再键入 factor(A)，再回车即可。

算术基本定理看起来似乎是一个很平凡的结果(因为很符合我们的直觉)，但是以后我们就会知道如果把整数的范围扩大，那么在别的类似于整数的数中，这个定理并不一定成立，这是很违反我们的直觉的，但这的确是一个事实。此外，从下面的定理的证明中，你也可以看出这个定理确实吸收了证明中的难点，用它证明某些结论显得轻而易举，而要不用，就很费劲，所以称它是“基本”定理还是很有道理的。

从素数基本定理和最大公约数、最小公倍数的定义显然可以立刻得出下面的定理：

定理 3.4.5　设 $a = p_1^{a_1}p_2^{a_2}\cdots p_n^{a_n}$，$b = p_1^{b_1}p_2^{b_2}\cdots b_n^{b_n}$，其中 a_i 和 b_i 都是非负整数，那么

$$(a,b) = p_1^{c_1}p_2^{c_2}\cdots p_n^{c_n}$$

$$[a,b] = p_1^{e_1}p_2^{e_2}\cdots p_n^{e_n}$$

其中 $$c_i = \min(a_i, b_i), e_i = \max(a_i, b_i), i = 1, 2, \cdots, n$$

由此定理和显然的等式 $\min(x, y) + \max(x, y) = x + y$ 立刻又可得出

$$(a, b)[a, b] = ab$$

因此 $$[a, b] = \frac{ab}{(a, b)}$$

如果你对比这里的证明和定理 3.3.15 的证明，你就会发现这里的证明简单多了（根本就是一个几乎是直接的推论）。下面这个定理又是一个用算术基本定理可以轻易推出，而要不用则颇费气力的例子。

定理 3.4.6 设 $(a, b) = 1, ab = c^k$，则 $a = u^k, b = v^k$，而且 $u = (a, c)$，$v = (b, c)$。

证明 设 $c = p_1^{c_1} p_2^{c_2} \cdots p_n^{c_n}$，则 $c^k = p_1^{c_1 k} p_2^{c_2 k} \cdots p_n^{c_n k}$。由算术基本定理（这个定理确定了 c^k 的因子的形式），我们可设

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}, b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$$

由条件 $ab = c^k$ 知 $a_i + b_i = kc_i (1 \leqslant i \leqslant n)$，而由 $(a, b) = 1$ 和定理3.4.5 又知 $\min(a_i, b_i) = 0 (1 \leqslant i \leqslant n)$，由上面两个式子立即得到 $a_i = 0, b_j = kc_i$ 或 $a_i = kc_i, b_i = 0$。

于是我们知道 a 和 b 的素因子分解式中的指数都只有两种情况，而且这两种情况发生的指标集在 a 和 b 中都是不相交且互补的。说得更明确些就是：设

$$I = \{1, 2, \cdots, n\}, A = \{i \mid a_i = kc_i, 1 \leqslant i \leqslant n\}, B = I \setminus A$$

则显然 $$A \cup B = I, A \cap B = \varnothing$$

因此

$$b_i = kc_i, i \in B, a = \prod_{i \in A} p_i^{kc_i} = u^k, b = \prod_{i \in B} p_i^{kc_i} = v^k$$

其中 $$u = \prod_{i \in A} p_i^{c_i}, v = \prod_{i \in B} p_i^{c_i}$$

由此就得出

$$(a, c) = \Big(\prod_{i \in A} p_i^{kc_i}, \prod_{1}^{n} p_i^{c_i}\Big) = \prod_{i \in A} p_i^{c_i} \Big(\prod_{i \in A} p_i^{(k-1)c_i}, \prod_{i \in B} p_i^{c_i}\Big) = \prod_{i \in A} p_i^{c_i} = u$$

或 $u = (a, c)$，同理 $v = (b, c)$。这就证明了定理的结论。

但是我们马上又会提出一个问题，就是素数究竟是有限的还是无限的？如果全体素数是有限的，那么好多问题就变得起码原则上是很简单的。比如分解质因数问题，我们所要做的就将只不过是把这有限的全体素数找出来，印成表，然后依次去试验哪些素数能整除我们想要分解的数而已。

其实，我们想到的这个问题，古代希腊有一个叫欧几里得的数学家早就想过了，并且用一种很巧妙的方法给出了答案。当然在此之前，人们用实验的方法也已经发现了很多素数，并且猜想素数应该是无穷的，但是猜想毕竟不能算是

严格的证明。

欧几里得的方法是一种程序式的计算，也就是说，它给出一种计算的程序，按照这种程序就可以造出无穷多的素数，于是全体素数当然就是无穷的了。下面我们就给出这个证明。

定理 3.4.7 素数是无穷的。

证明 通过定义直接验算，我们已知 2,3,5 等都是素数，其中除了 2 之外，其余的素数都是大于 2 的奇数，或是具有形式 $2k+1$ 的数。现在任选一个除 2 之外的素数 p_1，令 $q_1 = p_1, q_2 = 2p_1 + 1$，那么显然 $(q_1, q_2) = (p_1, 2p_1 + 1) = (p_1, 1) = 1$，因此 q_1, q_2 是互素的。

现在考虑两种情况：

(1) q_2 是一个合数，那么由于 q_2 具有形式 $2k+1$，因此它的因子中必至少有一个也具有这种形式（实际上是 q_2 的全体真因数都必须具有这种形式，不过我们为了给习题中的问题示范，只用到这点）。也就是说 q_2 的具有形式为 $2k+1$ 的真因子的集合 A 是非空的集合。那么因此根据自然数的最小数原理，这个集合中的全体自然数就有一个最小的数 p_2。p_2 必定是一个素数，否则，我们将得出 p_2 又有一个形式为 $2k+1$ 的真因子 r，r 显然也是 q_2 的真因子，而这与 p_2 的最小性相矛盾。由于 $(q_1, q_2) = 1$，所以 $p_2 \neq p_1$。于是在这种情况下，我们就找到了一个新的不同于我们已选定的素数 p_1 的素数 p_2。

(2) q_2 是一个素数，那么显然 q_2 本身就是一个新的不同于我们已选定的素数 p_1 的素数。

综合上述讨论，无论发生哪种情况，我们都可以找到一个新的不同于我们已选定的素数 p_1 的素数 p_2。

现在令 $q_3 = 2p_1p_2 + 1$，于是与以上的证明同理有 $(q_2, q_3) = 1$。重复上面的证明，我们又可以找到一个一个新的不同于我们已知的素数 p_1, p_2 的素数 p_3。

再令 $q_4 = 2p_1p_2p_3 + 1, \cdots$，依次类推，我们就可以找出无穷多个素数。

比如，令 $q_1 = p_1 = 3$，那么 $q_2 = 2 \cdot 3 + 1 = 7, p_2 = 7, q_3 = 2 \cdot 3 \cdot 7 + 1 = 43, p_3 = 43, q_4 = 2 \cdot 3 \cdot 7 \cdot 43 + 1 = 1\,807, p_4 = 13, \cdots$

你也可以令 $q_1 = p_1 = 5$，这时 $q_2 = 2 \cdot 5 + 1 = 11, p_2 = 11, q_3 = 2 \cdot 5 \cdot 11 + 1 = 111, p_3 = 3, q_4 = 2 \cdot 5 \cdot 11 \cdot 3 + 1 = 331, p_4 = 331, \cdots$

习题 3.4

1. 证明：$N = \dfrac{5^{125} - 1}{5^{25} - 1}$ 是一个合数。

2. (1) 证明：$2^{4n+2} + 1 = (2^{2n+1} - 2^{n+1} + 1)(2^{2n+1} + 2^{n+1} + 1)$；

   (2) 分解因数 $2^{58} + 1$。

3. 证明：$2^{32}+1$ 是一个合数。

4. 证明：若 2^n+1 是一个素数，则 n 必是 2 的方幂。

5. 设 $n>0, a\neq b, n\mid(a^n-b^n)$，则 $n\mid\frac{a^n-b^n}{a-b}$。

6. 设 a,b,c,d 都是正整数，且 $ab=cd$，证明：$a^3+b^3+c^3+d^3$ 必是一个合数。

7. (1) 设 a,b,c,d 都是正整数，且 $ab=cd$，证明：$a^2+b^2+c^2+d^2$ 必是一个合数；

(2) 证明：若自然数 n 可以用两种不同的方法表示成两个整数的平方和，则 n 必是一个合数。

8. (1) 验证等式 $533=23^2+2^2=22^2+7^2$，$1\,073=32^2+7^2=28^2+17^2$；

(2) 把 533 和 1 073 分解成质因数的乘积。

9. 证明：任给自然数 n，必存在 n 个都是合数的连续的自然数。

10. (1) 证明：任一形如 $3k-1, 4k-1, 6k-1$ 的正整数，必有同样形式的素因数；

(2) 证明：有无穷多个形如 $4k-1$ 的素数；

(3) 证明：有无穷多个形如 $6k-1$ 的素数。

3.5 方程式的整数解

上过中学的读者对方程式和如何解方程都不会陌生。我们在第一章谈数是如何产生时，就已经说过，各种新的数的产生，在很大程度上是为了使以前没有解的方程能够有解。然而虽然随着各种新的数的产生，我们能不断地扩大方程式的解的范围，我们又不止一次地一遍又一遍地要回到最原始产生的数，即整数中去研究方程式的解。这一方面是直接来源于实际的问题，因为在实际问题中，的确存在着只取整数才有意义的数量，例如人的个数，活的动物的个数，钞票的张数，物体的个数等等；另一方面，在理论上和美感上，也对方程式的整数解有特殊的兴趣。这可能是来源于我们最先开始认识的数就是整数，人总是这样，对最先接触的东西印象特别深，并且深深地"眷恋"它，用这种观点可以解释人的很多行为。我自己就不断地体会过获得方程式的一个整数解时的愉快感觉，好像我的许多同学也有过这种体会，在我们上小学，中学时，如果解方程时，所得的解恰好是一个整数，就会有一种真带劲，或者运气真好的愉快感觉。直到现在，我在解方程时，仍然有这种偏好。我想没有几个人是特别喜欢好不容易才求出来的方程式的解是一个要用很多符号表示出来的复杂的式子。如果一个人

有这种偏好，恐怕大家都会觉得这个人很怪。

刚才我们提到在实际中的确存在着要求解必须取整数的问题。实际上，从古代到现在，无论中外，无论是在民间的流传还是研究数学的书籍中都可以找到这种问题。下面我们就来举一个这种问题的例子。

例 3.5.1 有若干个不同规格的油桶，大的能装 7 kg，小的能装 5 kg，现有 80 kg 的油恰好装满这些油桶，问大小油桶各几个？

解 可以设要用大油桶 x 个，小油桶 y 个，那么根据题意就可得到一个方程

$$7x + 5y = 80$$

这个方程我们都知道是一个二元一次方程，一般来说，它有无数个解。比如如果用 x 来表示 y，那么我们就可以得出一个明显的表示式

$$y = \frac{80 - 7x}{5}$$

在上面这个式子里，每给 x 一个特殊值，就可以相应地得到 y 的一个特殊值，如此，给出许多 x 的特殊值，就可以得到想要多少就有多少的解。例如，用这种方法，我们可以得出如下的表格：

x	-1	1	2	3	4
y	$\frac{87}{5}$	$\frac{73}{5}$	$\frac{66}{5}$	$\frac{59}{5}$	$\frac{52}{5}$

但是上面表中所列出的解都不符合要求，因为我们所要解决的问题本身的性质要求 x 和 y 都是整数，而且还应是非负的整数。加上这个要求之后，这个方程得符合要求的解就不是无限多了。像这种要求解要限制在某种特定的数中例如正整数、非负整数、有理数中的求解方程问题就称为不定方程，对不定方程的研究形成了整数研究中的一个专门的，十分有兴趣的特殊领域。这一领域至今仍吸引着许多人的兴趣，他们之中既包括普通的数学爱好者，也有专门的研究者，本书作者在北京以及河南的农村都发现有的农民根本没有上过学，也不识字，但是当他们得知我是学数学的老师后，有的人竟会向我提出在他们之间世代口头流传的趣味数学问题，而这些问题大部分是不定方程问题。可以说，这是一个雅俗共赏的领域。无论谁对这种问题感兴趣，我相信他都可以在这一领域中找到自己的乐趣。

具体到我们所提出的问题，我们可以把这个方程写成

$$7x = 80 - 5y = 5(16 - y)$$

由此得出 $7 \mid 5(16 - y)$，$x = \frac{5(16 - y)}{7}$，而由于 $(5,7) = 1$，因此，必须 $7 \mid (16 - y)$，由此得出

$$16 - y = 7m$$

或
$$y = 16 - 7m$$

这就好办了，因为现在 y 的系数是1，所以你任给 m 一个整数值，就会自动得到一个 y 的整数值，这样我们就可以求出所有适合要求的整数解了（只要使 $m \geqslant 0, 16 - 7m > 0$ 即可，也就是只要令 $m = 0,1,2$ 即可）。这些解就是 $x = 0, y = 16, x = 5, y = 9$ 或 $x = 10, y = 2$。

但是在解这种方程时，我们的运气不见得每次都是这样好，比如看下面这个问题：

例3.5.2 把一张5块钱的人民币换成5角、2角和5分的钱，使得纸币的张数和分币的个数加起来是20。

解 为了对上面的问题列出方程，我们设所换成的钱中有 x 个5分的硬币，y 张2角的纸币和 z 张5角的纸币。于是根据题意就可得出

$$5x + 20y + 50z = 500$$
$$x + y + z = 20$$

现在把第一个方程两端的公约数5约去，并用约过的方程减去第二个方程就得到

$$3x + 9y = 80$$

到这时，我们立刻可以看出，上述方程是不可能有整数解的，因为它的左端是3的倍数，而右端不是。因此原来的问题也不可能有整数解。但是这一点一开始并不是可以明显看出的。在民间流传的不定方程问题中，有一些就是没有解的，而且当地人经常会用这种问题来考验你，当你告诉他们这个问题无解时，他们往往先要说你算错了，这是一种心理讹诈，有的人就被他们吓回去了。作者在河南省太康县文教局工作时就碰到过这种事，当时文教局的一个姓汪的会计就给我出了一个这种问题，列出方程来也是两个三元一次方程，化到最后则是一边是2的倍数，一边不是。但当我告诉他这个问题无解时，他先是大喊一声"啥，啥叫无解？"在我耐心地向他解释无解的含义之后，他十分肯定地说："不对，你肯定算错了。"在我又仔细检查了一遍所有的式子后，我也十分肯定地坚持说这一问题不可能有解，并且指出，为了证明我是错的，就应该由他而不是我来说出这个问题的解是什么。经过几番抬杠和旁边看热闹的人对我的论点的支持后，他不得不承认这一问题确实没有解。并且说："老冯还是真正有学问的，我为什么这么说呢，因为这是一个复比例问题，而不是所有的人都知道复比例问题不是每次都有解的。"可见他早知道这个问题无解，先前的表现一直是在诈我。而且他对这个问题的理解与我完全不同，他是从复比例问题并不是每次都有解的这一点上来考我的，而我至今不懂得或者说可能学过但是早就忘了什么叫复比例问题了。

另一件更滑稽的事是在一次县里开什么会期间，有一位我忘了是语文老师还是干部的人，反正这个人是不懂多少数学知识的，来问我如何把 100 个豆子分在 9 个碗里，使得每个碗里的豆子都是单数。我立刻看出这个问题是不可能有解的。但是与文教局的那位姓汪的会计不同，这个人是不认为这个问题是无解的。而且你无法使他相信这一点，因为他除了能理解单数、双数这样的概念外，再向他进行其他任何解释和推理都是极为困难的。比如，当我试图向他解释，单数加上单数必定得到一个双数，而双数加上一个单数必定得到一个单数时，他表示无法理解，因此最后我没有办法让他相信这一问题不可能有解答，而他则坚信是我不会找出这一解答，而某个高人肯定能找出来。

我们再来考虑一个问题。

例 3.5.3 试求一个自然数，使得这个自然数被 3 除余 2，被 5 除余 3。

解 设所求的数为 x，x 被 3 除所得的商为 y，而被 5 除所得的商为 z，那么由带余数除法就可列出下列方程

$$x = 3y + 2 = 5z + 3$$

由上面的方程就得出

$$3y = 5z + 1$$

或者

$$y = \frac{5z + 1}{3}$$

用观察法很容易立刻看出一个解，即 $z = 1, y = 2, x = 8$。

为了求出其余的解，我们令 $z = 1 + u$，把 z 代入方程 $3y = 5z + 1$ 之中就得到

$$5u = 3y - 6 = 3(y - 2)$$

由此得出 $5 \mid 3(y - 2)$，$u = \dfrac{3(y - 2)}{5}$，而由于 $(3,5) = 1$，因此，必须 $5 \mid (y - 2)$，由此得出 $y - 2 = 5m$，或 $y = 5m + 2$。把这个式子代回去，就可以逐步得到

$$u = 3m, z = 3m + 1, x = 15m + 8$$

于是在这个问题中，我们发现可以得到无穷多组符合要求的整数解。

通过上面 3 个问题，我们就认识到在解一个形如二元一次方程的不定方程时，我们有可能碰到各种不同的情况：所要解的问题也许会根本没有解，也许会有无穷多个解，也可能只有有限的几个解，甚至是唯一的解。

现在我们来考虑这种问题的一般提法和解法。一个二元的一次不定方程的一般形式是

$$ax + by = c$$

其中，a, b, c 都是整数。虽然在很多实际问题中，要求解必须是正整数，但是正如我们在第一章有关负数的起源的内容中就已经指出的那样，许多问题如

果只限于在正整数范围内讨论，将变得极为繁琐，要分很多种情况并且得不到统一的表述。所以在讨论一般的二元的一次不定方程时，我们首先在全体整数的范围内讨论，以后需要时，再回到正整数范围内。以后我们仍会遇到这种情况，就是虽然你要解决的问题是在某一种比较特殊的数的范围内，但是在解决这一问题时，你必须先在一个更大的范围里讨论这一问题，待有了一般结论后，再回到我们所需要的某一种比较特殊的数的范围内去。

设 $d=(a,b)>1$，首先我们指出，如果 $d\nmid c$，那么就像例3.5.2中最后得出的方程 $3x+9y=80$ 那样，问题不可能有解，即使不限于正整数范围内也是这样。因为这时方程的一端是 d 的倍数，而另一端不是，因此两端不可能相等。于是我们得出：

引理 3.5.1 设 $d=(a,b)>1$，那么方程 $ax+by=c$ 有解的必要条件是 $d\mid c$。

因此，以后我们只须在条件 $(a,b)=1$ 的条件下考虑上述方程即可(因为如果 $d=(a,b)>1, d\mid c$，我们只须在方程两边同时除以 d，即可把原来的方程化为 $(a,b)=1$ 的情况)。其次，我们指出成立下述引理：

引理 3.5.2 如果知道了方程 $ax+by=c$ 的一组特殊解 (x_0,y_0)，那我们就可以写出这个方程的无穷多组解。

证明 由引理的条件知 $ax_0+by_0=c$，因此由等式

$$a(x_0-bt)+b(y_0+at)=ax_0+by_0=c$$

或等式

$$a(x_0+bt)+b(y_0-at)=ax_0+by_0=c$$

可以看出当 t 不同时，(x_0-bt,y_0+at) 或 (x_0+bt,y_0-at) 就给出方程 $ax+by=c$ 的无穷多组解。其实，只要把 t 换成 $-t$，就可以把上面的一种解的公式变成另一种，因此我们以后只要在上述两种公式中任选一种即可。

下面，我们证明，如果方程 $ax+by=c$ 有解，并且 (x_0,y_0) 是它的一组特殊解，那么它的所有解就都可以由公式 $x=x_0+bt, y=y_0-at$ 表出，其中 t 是一个任意整数。初一看，我们将要证明的结论和上面我们已证明过的引理 3.5.2 很相像，但是我们要指出这两个命题是完全不一样的，例如，只要你有足够的耐心，就可以用乘法验证当 s,t 是任意整数时，公式

$$x=1-(s-3t)(s^2+3t^2)$$
$$y=-1+(s+3t)(s^2+3t^2)$$
$$z=s+3t-(s^2+3t^2)^2$$
$$w=-s+3t+(s^2+3t^2)^2$$

就给出了方程

$$x^3+y^3=z^3+w^3$$

的无穷多组整数解。然而，你也可以验证，$x=1, y=12, z=9, w=10$ 满足上

述方程，但是这组解却不能用上述公式表示出来。(顺便说一下，$1^3+12^3=9^3+10^3=1\ 729$，而 1 729 是最小的能用两种方式表示成立方和的正整数)

引理 3.5.3 设 $ab\neq 0$，$(a,b)=1$，且 (x_0,y_0) 是方程 $ax+by=c$ 一组特殊解，那么方程 $ax+by=c$ 的所有解就都可以由公式 $x=x_0+bt$，$y=y_0-at$ 表出，其中 t 是一个任意整数。

证明 设 (r,s) 是方程 $ax+by=c$ 一组任意解，则由 (x_0,y_0) 和 (r,s) 的定义就有 $ax_0+by_0=c$，$ar+bs=c$。因此把两式相减就得到

$$a(x_0-r)+b(y_0-s)=0$$

或者

$$a(x_0-r)=-b(y_0-s)$$

故 $a\mid b(y_0-s)$，但是由于 $(a,b)=1$，因此必须 $a\mid(y_0-s)$，这就得出存在一个整数 t 使得 $y_0-s=at$，而 $s=y_0-at$，把 $s=y_0-at$ 代入方程 $a(x_0-r)+b(y_0-s)=0$ 就得到 $r=x_0+bt$，这就证明了引理。

最后我们再指出如果知道了方程 $ax+by=1$ 的一组特殊解 (x_0,y_0) 就可以知道方程 $ax+by=c$ 的一组特殊解。

引理 3.5.4 设 (x_0,y_0) 是方程 $ax+by=1$ 的一组特殊解，那么 (cx_0,cy_0) 就是方程 $ax+by=c$ 的一组特殊解。

证明 由等式 $a(cx_0)+b(cy_0)=c(ax_0+by_0)=c$ 即知引理成立。

根据以上几个引理，在方程 $ax+by=c$ 满足有解的必要条件的情况下(也即条件 $(a,b)=1$)，只要求得方程 $ax+by=1$ 的一组特殊解，我们就可求得方程 $ax+by=c$ 的所有解。因此现在全部问题即归结为如何求得方程 $ax+by=1$ 的一组特殊解。关于这个问题，可以有两个思路。第一个就是像在例 3.5.1 中那样，通过变量替换设法把其中一个未知数的系数变为 1，一旦做到了这一点，便不难求出所得方程的一组特殊解了，然后再逐步换回原来的变量，就可得出 $ax+by=1$ 的一组特殊解了。

例 3.5.4 试求出方程 $331x-169y=5$ 的所有整数解。

解 首先由于 $(331,169)=1$，因此这个方程是符合有解的必要条件的。我们先设法求出方程 $331x-169y=1$ 的一组特殊解。为此，我们设法把方程的系数通过变量替换变小。用较小的系数 169 去除较大的系数 331，由带余数除法得 $331=169+162$ 或者 $331x=169x+162x$。现在可以将原来的方程改写为

$$169x+162x-169y=1$$

或者

$$162x+169(x-y)=1$$

现在引入一个新的未知数 $x_1=x-y$，我们就得到一个系数比原来小的方程式 $162x+169x_1=1$，再用这个方程式中较小的系数去除较大的系数即得

$$169x_1=162x_1+7x_1$$

或

$$162(x+x_1)+7x_1=1$$

再引入一个新的未知数 $x_2 = x + x_1$，就得到一个系数更小的方程式 $162x_2 + 7x_1 = 1$，再用这个方程式中较小的系数去除较大的系数即得

$$162x_2 = 7 \cdot 23x_2 + x_2$$

或者

$$x_2 + 7(23x_2 + x_1) = 1$$

最后再设 $x_3 = 23x_2 + x_1$，我们就得到一个有一个系数为 1 的方程式

$$x_2 + 7x_3 = 1$$

或者

$$x_2 = 1 - 7x_3$$

现在，随便给 x_3 一个特殊值，就可得到 x_2 的一个特殊值，逐步替换回去就可得到原来的方程的一组特殊解了。例如我们不妨就令 $x_3 = 0$，就可逐步得出

$$x_2 = 1, x_1 = x_3 - 23x_2 = 0 - 23 = -23, x = x_2 - x_1 = 1 - (-23) = 24$$

$$y = x - x_1 = 24 - (23) = 47$$

经验算确实有 $331 \cdot 24 - 169 \cdot 47 = 1$。因而方程 $331x - 169y = 5$ 的一组特殊解就是 $x = 5 \cdot 24 = 120, y = 5 \cdot 47 = 235$。而方程 $331x - 169y = 5$ 的全部整数解就可写成

$$x = 120 + 169t, y = 235 - 331t$$

我们不难看出，上述过程的实质就是在对 331 和 169 做辗转相除法，而由于 $(331,169) = 1$，因此根据辗转相除法的做法，我们最后一定可以把其中一个未知数的系数化为 1。

第二个思路还是辗转相除法，不过不是通过上面所作的一系列变量替换，而是直接应用辗转相除法。由于 $(331,169) = 1$，因此在辗转相除法的算式中，最后一个余数 r_n 一定等于 1，而由定理 3.3.7 可知

$$Q_n a - P_n b = (-1)^{n-1} r_n = (-1)^{n-1}$$

我们就可直接得出方程 $331x - 169y = 1$ 的一组特殊解。综合上述引理就得出：

定理 3.5.1 设 $ab \neq 0, d = (a,b)$，则

(1) 当 $d \nmid c$ 时，方程 $ax + by = c$ 无整数解；

(2) 设 (x_0, y_0) 是方程 $ax + by = c$ 的一组特殊解，则方程 $ax + by = c$ 的所有整数解可由公式 $x = x_0 + bt, y = y_0 - at$ 表出，其中 t 是一个任意整数；

(3) 设 $(|a|, |b|) = 1$，由带余数除法，成立以下等式

$$|a| = bq_1 + r_1, 0 < r_1 < b$$

$$|b| = r_1 q_2 + r_2, 0 < r_2 < r_1$$

$$\vdots$$

$$r_{n-2} = r_{n-1} q_n + r_n, 0 < r_n < r_{n-1}$$

$$r_{n-1} = r_n q_{n+1}, r_n = 1$$

又设

$$P_0 = 1, P_1 = q_1, \cdots, P_k = q_k P_{k-1} + P_{k-2}$$
$$Q_0 = 0, Q_0 = 1, \cdots, Q_k = q_k Q_{k-1} + Q_{k-2}$$
$$k = 2, 3, \cdots, n$$

那么下列四组数(cQ_n, cP_n),$(cQ_n, -cP_n)$,$(-cQ_n, cP_n)$,$(-cQ_n, -cP_n)$之中,必有一组是方程 $ax + by = c$ 的一组特殊解。

例 3.5.5 求出方程式 $127x - 52y + 1 = 0$ 的所有整数解。

解 所要求解的方程可化为 $127x - 52y = -1$,$(127, 52) = 1$,$c = -1$;对 127 和 52 做辗转相除法得到

$$127 = 2 \cdot 52 + 23, q_1 = 2$$
$$52 = 2 \cdot 23 + 6, q_2 = 2$$
$$23 = 3 \cdot 6 + 5, q_3 = 3$$
$$6 = 1 \cdot 5 + 1, q_4 = 1$$
$$5 = 5 \cdot 1, n = 4$$
$$P_0 = 1, P_1 = q_1 = 2, P_2 = q_2 P_1 + P_0 = 2 \cdot 2 + 1 = 5$$
$$P_3 = q_3 P_2 + P_1 = 3 \cdot 5 + 2 = 17, P_4 = q_4 P_3 + P_2 = 1 \cdot 17 + 5 = 22$$
$$Q_0 = 0, Q_1 = 1, Q_2 = q_2 Q_1 + Q_0 = 2 \cdot 1 + 0 = 2$$
$$Q_3 = q_3 Q_2 + Q_1 = 3 \cdot 2 + 1 = 7, Q_4 = q_4 Q_3 + Q_2 = 1 \cdot 7 + 2 = 9$$

而 $127 \cdot 9 - 52 \cdot 22 = -1$,于是方程式 $127x - 52y + 1 = 0$ 的所有整数解即为

$$x = 9 - 52t, y = 22 - 127t$$

或

$$x = 9 + 52t, y = 22 + 127t$$

在实际问题中经常会出现多于两个变元的一次不定方程和方程组。我们不可能在这本书中给出这类问题的一般解答,因为这不可避免地要引进许多线性代数的概念和理论。我们只在这里提一下两类比较特殊的问题。

一类问题是求一个多元一次不定方程的整数解,即形如

$$a_1 x_1 + a_2 x_2 + \cdots + a_n x_n = N, n > 2$$

的方程的解。很明显这类方程可以化为二元一次不定方程的情况来加以研究。例如,如果上述方程的 n 个系数中,有某两个是互素的,不失一般性,不妨设 $(a_1, a_2) = 1$(否则可以通过调换系数的位置来化成这种情况)。那么就可以把上述方程化为

$$a_1 x_1 + a_2 x_2 = N - a_3 x_3 - \cdots - a_n x_n$$

这时只要把 $x_3, x_4, \cdots, x_n$ 看成自由未知量(即可以随便取任何整数值的变量),并且把它们看成已知的常数,就可以像解普通的二元一次不定方程那样类求解了。而如果上述系数中任何两个都不互素,则由定理 3.3.6 可知 $d = (a_1,$

$a_2, \cdots, a_n) > 1$。如果 $d \nmid N$，则显然原方程就没有整数解，如果 $d \mid N$，则用 d 去除方程的两边，就可把原方程化成 $d = 1$ 的情况，这时一定存在两个系数 a_i, a_j 使得 $(a_i, a_j) = 1$，因而按照上面我们讲过的办法一定可以求出原方程的无穷多组整数解。这就得出：

定理 3.5.2 设 $d = (a_1, a_2, \cdots, a_n)$，那么不定方程

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = N, n > 2$$

有解的充分必要条件是 $d \mid N$。

例 3.5.6 求 $9x + 24y - 5z = 1\,000$ 的所有整数解。

解 由于 $(9, 24, -5) = 1$，因此原方程有解。通过观察发现 $(9, -5) = 1$，且系数的绝对值较小，因此我们把方程化为 $-9x - 5z = 1\,000 - 24y$，用例3.5.4或例3.5.5中的方法，我们可以求得 $9 \cdot (-1) - 5 \cdot (-2) = 1$，因此原方程组的所有整数解可以表示成

$$x = -(1\,000 - 24y) + 5t, z = -2(1\,000 - 24y) + 9t$$

其中，y 和 t 是任意整数。

另一类问题是求两个三元一次方程组成的三元一次方程组的整数解（更一般的是求 $n-1$ 个 n 元一次方程组成的 n 元一次方程组的整数解）。也就是求形如

$$a_1x + b_1y + c_1z = e_1$$

$$a_2x + b_2y + c_2z = e_2$$

的方程组的所有整数解。从例 3.5.2 中我们已知，这种方程不一定有解。我们不准备详细地讨论这种方程所可能出现的每一种细节，只给出一种把它化成二元一次不定方程以进行讨论的方法。首先我们检查在 a_1, a_2 或者 b_1, b_2 或者 c_1, c_2 这三组数之中是不是有一组是互素的，如果有，比如说是 $(c_1, c_2) = 1$，那么用例 3.5.4 或例 3.5.4 中的方法，我们就可以求出两个数 λ 和 μ 使得 $\lambda c_1 + \mu c_2 = 1$，用 λ 和 μ 分别去乘原方程组中的两个方程，并把它们相加，就可以得出

$$(\lambda a_1 + \mu a_2)x + (\lambda b_1 + \mu b_2)y + z = \lambda e_1 + \mu e_2$$

或者 $$z = \lambda e_1 + \mu e_2 - (\lambda a_1 + \mu a_2)x - (\lambda b_1 + \mu b_2)y$$

把这个方程代入原方程组中的任何一个方程，就可以得出一个我们已讨论过的二元一次不定方程，然后我们就可以利用本节已讲过的内容对这个二元一次不定方程进行讨论了。这种情况属于只须讨论一次的情况。还有一种情况就是 a_1, a_2 或者 b_1, b_2 或者 c_1, c_2 这三组数都不是互素的，这时我们可以挑选一组比较简单的，比如说 c_1, c_2。设 $d = (c_1, c_2) > 1$，那么仍用例3.5.4或例3.5.5中的方法，我们就可以求出两个数 λ 和 μ 使得 $\lambda c_1 + \mu c_2 = d$，用 λ 和 μ 分别去乘原方程组中的两个方程，并把它们相加，就可以得出

$$(\lambda a_1 + \mu a_2)x + (\lambda b_1 + \mu b_2)y + dz = \lambda e_1 + \mu e_2$$

或者 $$z=\frac{\lambda e_1+\mu e_2-(\lambda a_1+\mu a_2)x-(\lambda b_1+\mu b_2)y}{d}$$

把这个式子代入原方程中的任意一个(比如说第一个),就可得出一个关于 x,y 的二元一次不定方程

$$(da_1-c_1(\lambda a_1+\mu a_2))x+(db_1-c_1(\lambda b_1+\mu b_2))y=(d-c_1)(\lambda e_1+\mu e_2)$$

这时可按照前面讲过的内容对上面的方程进行第一次判定,如果他有解,那么用例 3.5.4 或例 3.5.5 中的方法,就可求出它的一组特解(x_0,y_0),并用这组特解表示出上面这个关于 x,y 的二元一次不定方程的所有整数解

$$x=x_0-(db_1-c_1(\lambda b_1+\mu b_2))t$$

$$y=y_0+(da_1-c_1(\lambda a_1+\mu a_2))t$$

把这组解代入到方程

$$(\lambda a_1+\mu a_2)x+(\lambda b_1+\mu b_2)y+dz=\lambda e_1+\mu e_2$$

中,经过化简,就可得到一个关于 t 和 z 的二元一次不定方程

$$c_1(\mu(a_1b_2-a_2b_1)t+z)=\lambda e_1+\mu e_2-a_1x_0-b_1y_0$$

这时还要进行第二次判定,即判定 c_1 是否能整除 $\lambda e_1+\mu e_2-a_1x_0-b_1y_0$,如果不能,则显然原方程无解,如果能,就可得出原方程的所有整数解如下

$$x=x_0-(db_1-c_1(\lambda b_1+\mu b_2))t$$

$$y=y_0+da_1-c_1(\lambda a_1+\mu a_2))t$$

$$z=\frac{\lambda e_1+\mu e_2-a_1x_0-b_1y_0}{c_1}-\mu(a_1b_2-a_2b_1)t$$

下面我们来解一个由我国古代数学家张邱建所著的数学书籍《张邱建算经》中的问题。

张邱建,中国数学家,清河人,生于履历不详,据《宋史·礼志》记载为晋人.

例 3.5.7 “鸡翁 1,值钱 5,鸡母 1,值钱 3,鸡雏 3,值钱 1。百钱买白鸡,问鸡翁母雏各几何?”

解 设有鸡翁 x 个,鸡母 y 个,鸡雏 z 个,则根据题意可列出方程如下

$$5x+3y+\frac{z}{3}=100$$

$$x+y+z=100$$

在上面的方程组中,第二个方程里所有的未知数的系数已经都是 1,所以这是一个只须判定一次并解一次的不定方程。我们就选 z 作为已知量,从第二个方程得

$$z=100-x-y$$

把 z 的表达式代入第一个方程并化简得

$$7x+4y=100$$

由于$(7,4)=1$,所以上面的方程有整数解。用例3.5.4或例3.5.5中的方法或用

观察法看出

$$7\cdot(-1)+4\cdot 2=1$$

由此可知，方程 $7x+4y=100$ 的整数解可写成

$$x=-100+4t,y=200-7t$$

的形式，再把上面的表达式代入 $z=100-x-y$ 中，即得出原方程的所有整数解为

$$x=-100+4t,y=200-7t,z=3t$$

为了求出符合题意的整数解，还必须求不等式组 $x\geqslant,y\geqslant 0,z\geqslant 0$ 的整数解。解这个不等式，我们共获得以下 4 个解：$t=25,26,27,28$，这四个解对应了原方程组的四组解如下

$$\begin{cases}x=0\\y=25,\\z=75\end{cases}\begin{cases}x=4\\y=18,\\z=78\end{cases}\begin{cases}x=8\\y=11,\\z=81\end{cases}\begin{cases}x=12\\y=4\\z=84\end{cases}$$

例 3.5.8 求出方程组 $\begin{cases}4x+6y+15z=100\\6x+9y+10z=100\end{cases}$ 的所有非负整数解。

解 由于 $(4,6)=2,(6,9)=3,(15,10)=5$，因此我们不可能通过消元法把任何一个未知数的系数化为 1，故这是一个需要判定两次并解两次的不定方程组。

由于 $(4,6)=2$，故 x 的系数是比较简单的，通过观察法看出 $6-4=(4,6)=2$，因此用第二个方程减去第一个方程即得 $2x+3y-5z=0$ 或者 $x=\frac{5z-3y}{2}$。把 x 的表达式代入比如第一个方程，就得到 $z=4$，而 y 可暂时看成自由未知量，再把 y,z 代入 x 的表达式，就得出第二个不定方程 $2x+3y=20$，由于 $(2,3)=1$，因此这个不定方程仍然有解。通过观察法看出 $2\cdot 2+3\cdot(-1)=1$，因此方程 $2x+3y=20$ 的所有整数解可表为

$$x=40-3t,y=-20+2t$$

于是原方程组的所有整数解为 $x=40-3t,y=-20+2t,z=40$。为了求出原方程组的非负整数解，我们还需求不等式组 $x\geqslant 0,y\geqslant 0,z\geqslant 0$ 的整数解。解这个不等式，我们共获得以下 4 个解 $t=10,11,12,13$，这四个解对应了原方程组的四组解如下

$$\begin{cases}x=10\\y=0\ ,\\z=40\end{cases}\begin{cases}x=7\\y=2\ ,\\z=40\end{cases}\begin{cases}x=4\\y=4\ ,\\z=40\end{cases}\begin{cases}x=1\\y=6\\z=40\end{cases}$$

关于一次不定方程的话题我们就谈到这为止。

几何问题经常可以引出各种其他的不定方程问题，而且一般都不是一次的。比如在一定条件下三角形的边长何时可取整数就是一类很有兴趣的问题。

这种问题包括：求出所有边长和面积都是正整数的三角形；求出一个角是 120°或 60° 的有整数边长的三角形。由余弦定理，后一问题就等价于求出二次不定方程

$$x^2 + y^2 + xy = z^2$$

或

$$x^2 + y^2 - xy = z^2$$

的整数解。90° 角是一个让人感到特别"好"的角。如果考虑求出所有边长为整数的直角三角形的问题，就可以引出一个特别简单的二次不定方程

$$x^2 + y^2 = z^2$$

其中，x 和 y 表示直角三角形的两条直角边，而 z 则表示直角三角形的斜边。在我国古代西汉时期(公元前206年 ~ 公元8年)的数学书籍《周髀算经》中，已经有"句广三，股修四，径隅五"("句"是"勾"的古代写法)的记载，这句话被后来的中国数学家压缩成"勾三，股四，弦五"，这就是说我国古代的数学家至少在公元前就已知道了上述方程的一组整数解：$x = 3, y = 4, z = 5$。刘徽后来在《九章注》(263年)中又有 $5^2 + 12^2 = 13^2, 8^2 + 15^2 = 17^2, 7^2 + 24^2 = 25^2, 20^2 + 21^2 = 29^2$ 的记载，由此可知在我国古代就已经知道方程 $x^2 + y^2 = z^2$ 的很多组整数解。现在我们通常又把这个方程的整数解称为勾股数，把直角三角形的三条边的边长必满足方程 $x^2 + y^2 = z^2$ 这一事实称为勾股定理(在西方通常把这个方程称为毕达哥拉斯定理)。下面我们就来研究这个方程的整数解。

首先注意显然 $x = 0, y = 0, z = 0$；$x = 0, y = \pm z$ 或 $x = \pm z, y = 0$ 都是 $x^2 + y^2 = z^2$ 的整数解，除此之外 $x^2 + y^2 = z^2$ 的每一组解都不包含零。其次如果 x, y, z 是方程 $x^2 + y^2 = z^2$ 的一组解，那么 $-x, -y, -z$ 也是方程 $x^2 + y^2 = z^2$ 的一组解，更一般的，设 d 是任一正整数，那么 dx, dy, dz 也是方程 $x^2 + y^2 = z^2$ 的一组解。因此我们以后不妨设 $x > 0, y > 0, z > 0$ 并且 $(x, y) = 1$(如果 $d = (x, y) > 1$，那么 $d \mid x, d \mid y$，因此 $d^2 \mid x^2, d^2 \mid y^2$，因此 $d^2 \mid (x^2 + y^2)$，即 $d^2 \mid z^2, d \mid z$，这时从方程两边约去 d 就可得到 $(x, y) = 1$)。下面我们先证明

引理 3.5.5 设正整数 $x > 0, y > 0, z > 0$ 并且 $(x, y) = 1$ 满足方程 $x^2 + y^2 = z^2$，那么 x, y 不可能都是奇数。

证明 用反证法，假如 x, y 都是奇数。那么不妨设 $x = 2p + 1, y = 2q + 1$，于是由计算得出

$$x^2 + y^2 = (2p + 1)^2 + (2q + 1)^2 = 4(p^2 + q^2 + p + q) + 2$$

最后所得出的这个数既不可能是一个偶数的平方(因为偶数的平方能被 4 整除，而这个数被 4 除余 2)，也不可能是一个奇数的平方(因为奇数的平方被 4 除余 1)。这就得出矛盾，所得的矛盾就证明了引理。

由这个引理我们又可推出以下引理：

引理 3.5.6 在 $(x, y) = 1$ 的条件下，方程 $x^2 + y^2 = z^2$ 的解中的 x 和 y 必

定一个是奇数，一个是偶数，而 z 一定是奇数。

证明　由引理3.5.5，x,y 不可能都是奇数，而由条件 $(x,y)=1$，它们也不可能都是偶数。因此必然是一奇一偶。由此又可推出 z 一定是一个奇数。

由上面的引理我们不妨设 x 是偶数，y 是奇数。于是我们可以写 $x=2u$，而将方程 $x^2+y^2=z^2$ 写成 $4u^2+y^2=z^2$ 或者 $4u^2=z^2-y^2$，最后的方程又可写成

$$4u^2=(z+y)(z-y)$$

由于 y 和 z 都是奇数，而两个奇数的和或者差必定是一个偶数，因此我们又可设

$$z+y=2v,z-y=2t$$

我们证明 v 和 t 必定是互素的，同时必定一个是偶数，另一个是奇数。实际上，用 v 和 t 来表示 z 和 y 就可得到 $z=v+t,y=v-t$。如果 $d=(v,t)>1$，那么显然 $d\mid z,d\mid y$，因此 $d^2\mid z^2,d^2\mid y^2,d^2\mid(z^2-y^2)$，也即 $d^2\mid x^2,d\mid x$，由此得出 $(x,y)>d>1$，而这与 $(x,y)=1$ 矛盾。另外 v 和 t 也不可能同时为奇数或同时为偶数，否则由 $z=v+t$ 就会得出 z 是一个偶数，而这与引理3.5.6中的断言 z 必定是一个奇数相矛盾。

把表达式 $z+y=2v,z-y=2t$ 代入方程 $4u^2=(z+y)(z-y)$ 中并化简就得到 $u^2=vt$。

再由定理3.4.6和表达式 $x=2u,z=v+t,y=v-t$ 即得到

定理3.5.3　方程 $x^2+y^2=z^2,x>0,y>0,z>0,(x,y)=1,2\mid x$ 的所有整数解可以表示成

$$x=2ab,y=a^2-b^2,z=a^2+b^2$$
$$a>b>0,(a,b)=1,a,b$$

之中一个是奇数，一个是偶数的形式。

而任意勾股数可以表示成 $x=2abn,y=(a^2-b^2)n,z=(a^2+b^2)n$ 的形式，其中 n 为任意整数。

我们在解上面的几种不定方程时除了首先做一些技术性的正规化工作外(比如不妨假定未知数是正的并且是互素的之类)，对一次不定方程主要就是研究如何把某个未知数的系数归一，这时辗转相除法起了相当大的作用。但是这个归一的办法在研究二次以上的不定方程时就没有多大用处了。在求一次不定方程和勾股数方程的整数解时，一个共同的主要手段就是定理3.3.8和定理3.3.9。除此之外，就没有什么有力的手段了。我们以后还要介绍一类称为贝尔方程的二次不定方程的解法。一般来说，对高于二次的不定方程不存在求解的一般方法，而且除了一些特殊的方程外，这些方程或者不存在任何整数解或者只存在有限组整数解。不过假如你已经知道一个不定方程只有有限组解，并能确定它的解的界限，那你倒不用再去研究如何求解的问题了，现代的计算技术

通常能帮助你迅速找出这些解。

在历史上，西方的数学家们在求出了方程 $x^2+y^2=z^2$ 所有整数解后，就立刻转向研究方程 $x^3+y^3=z^3, x^4+y^4=z^4, \cdots$ 乃至方程 $x^n+y^n=z^n$ 的整数解问题。结果一直到十七世纪中叶以前，都没有结果。到了十七世纪中叶，法国数学家费马对此问题发生了浓厚的兴趣。费马是他的家乡图卢兹城的著名社会活动家和法律家，但是他在业余时间热衷于研究数学问题，尤其是整数的问题。在他收藏的一个叫丢番图的数学家著的书的页边上，费马用拉丁语写了一段话："任何一个数的立方不能分解成两个立方之和，任何一数的四次方不能分解成两个四次方的和，或一般的，任何次的幂，除平方外，不可能分解成其他两个同次幂的和；我得到了这个断语的令人惊异的证明方法。但这页边太窄不容我将证明写出来。"所以后来就把证明方程 $x^n+y^n=z^n$ 没有正整数解的问题称为费马问题。但是人们在他的文稿或其传抄本中以及任何其他地方都没能找到这个证明。现在估计费马其实没能证明这个定理或者他自己认为证明了实际上是错的。但是费马在研究这一问题时创立了一种很有价值的方法叫做"无穷递降法"，他虽然没有能解决费马问题，但是这种方法在解决其他一些问题时（包括 $n=4$ 时的费马问题）却起到了关键性的作用。后来欧拉（1797 年）证明了方程 $x^3+y^3=z^3$ 和 $x^4+y^4=z^4$ 没有整数解；勒让德（1823 年）对 $n=5$ 证明了费马问题；拉梅与勒贝格（1840 年）对 $n=7$ 证明了费马问题；1849 年古默对一大批 n 证明了费马问题，并顺便证明了当 $n \leqslant 100$ 时，费马猜想都是正确的。

丢番图（Diophantus of Alexandria，活动于 250—275 前后），希腊数学家，生卒不详。

费马（Fermat, Pierre de, 1601—1665），法国数学家，生于法国南部图卢兹附近波蒙－德洛马涅，卒于卡斯特尔。

300 多年来，人们对此问题苦苦思索却一直找不到解答。1922 年，在黎曼的工作基础上，英国数学家莫德尔提出一个重要的猜想："设 $F(x,y)$ 是两个变数 x、y 的有理系数多项式，那么当曲线 $F(x,y)=0$ 的亏格（一种与曲线有关的量）大于 1 时，方程 $F(x,y)=0$ 至多只有有限组有理数。"1983 年，德国 29 岁的数学家法尔廷斯运用苏联沙法拉维奇在代数几何上的一系列结果证明了莫德尔猜想。这是费马大定理证明中的又一次重大突破。法尔廷斯因此获得了 1986 年的菲尔兹奖。

英国数学家怀尔斯仍采用代数几何的方法去攀登，他把别人的成果奇妙地联系起来，并且吸取了走过这条道路的攻克者的经验教训，注意到一条崭新迂回的路径，即 1988 年德国数学家费雷在研究日本数学家谷山和志村于 1955 年关于椭圆函数的一个猜想时发现的路线：如果谷山－志村猜想成立，那么费马大定理一定成立。

怀尔斯出生于英国牛津一个神学家庭，从小对费马大定理十分好奇和感兴趣，这条美妙的定理引导他进入了数学的殿堂。大学毕业以后，他开始了幼年的幻想，决心去圆童年的梦。他极其秘密地进行费马大定理的研究，守口如瓶，不透半点风声。

经过七年锲而不舍的努力，直到1993年6月23日怀尔斯才公开了他的研究结果。这天，英国剑桥大学牛顿数学研究所的大厅里正在进行例行的学术报告会。报告人怀尔斯作了长达两个半小时的发言。10点30分，在他结束报告时，他平静地宣布："因此，我证明了费马大定理。" 这句话像一声惊雷，把许多只要作例行鼓掌的手定在了空中，大厅顿时鸦雀无声。半分钟后，雷鸣般的掌声似乎要掀翻大厅的屋顶。英国学者顾不得他们优雅的绅士风度，忘情地欢腾着。

消息很快震动了全世界。各种大众传媒纷纷报道，并称之为"世纪性的成就"。人们认为，怀尔斯最终证明了费马大定理，这一事件被列入1993年世界科技十大成就之一。

可不久，传媒又迅速地报出了一个"爆炸性" 新闻：怀尔斯的长达200页的论文送交审查时，却被发现证明有漏洞。

怀尔斯在挫折面前没有止步，他用一年多时间修改论文，补正漏洞。这时他已是"为伊消得人憔悴"，但他"衣带渐宽终不悔"。1994年9月，他重新写出一篇108页的论文，寄往美国。论文顺利通过审查，美国的《数学年刊》杂志于1995年5月发表了他的这一篇论文。怀尔斯因此获得了1995～1996年度的沃尔夫数学奖。

希尔伯特（Hilbert，David，1862—1943），德国数学家，生于普鲁士柯尼斯堡，卒于格丁根.

经过300多年的不断奋战，数学家们世代的努力，费马问题终获解决。围绕费马大定理作出了许多重大的发现，并促进了一些数学分支的发展，尤其是代数数论的进展。现代代数数论中的核心概念"理想数"，正是为了解决费马大定理而提出的。难怪大数学家希尔伯特称赞费马大定理是"一只会下金蛋的母鸡"。

下面我们就具体来看一下如何用定理3.5.3和无穷递降法来证明 $n=4$ 时的费马问题。

定理 3.5.4　方程 $x^4+y^4=z^2$ 不存在正整数解。

证明　假定上述命题不真，即假定上述方程存在着至少一组正整数解，则可设这组解为

$$x_1>0,\ y_1>0,\ z_1>0$$

如果 $(x_1,y_1)>1$，则用 $(x_1,y_1)^4$ 去除方程 $x^4+y^4=z^2$ 的两边，即得到

$$\left(\frac{x_1}{(x_1,y_1)}\right)^4+\left(\frac{y_1}{(x_1,y_1)}\right)^4=\left(\frac{z_1}{(x_1,y_1)}\right)^2$$

这说明 $\left(\frac{x_1}{(x_1,y_1)},\frac{y_1}{(x_1,y_1)},\frac{z_1}{(x_1,y_1)^2}\right)$ 也是方程 $x^4+y^4=z^2$ 的一组正整数解，而且

$$\left(\frac{x_1}{(x_1,y_1)},\frac{y_1}{(x_1,y_1)}\right)=1$$

因此我们不妨设$(x_1,y_1)=1$。

类似于引理3.5.6,我们可以证明x^2,y^2这两个数中,必定一个是奇数,一个是偶数。不妨设x^2是偶数,于是由定理3.5.3即得

$$x_1^2=2ab,y_1^2=a^2-b^2,z_1=a^2+b^2$$

其中$a>b>0,(a,b)=1,a,b$之中一个是奇数,一个是偶数。因此x_1是偶数,y_1,z_2都是奇数。我们断言a必是一个奇数而b必是一个偶数。因为不然的话就会是a是一个偶数,b是一个奇数。故

$$a=2a_1,b=2b_1+1$$

$$y_1^2=a^2-b^2=4a_1^2-(2b_1+1)^2=4(a_1^2-b_1^2-b_1—1)+3$$

这说明y_1^2是一个被4除余3的数。但是另一方面,由y_1是一个奇数易证y_1^2必是一个被4除余1的数,这就得出矛盾。所得的矛盾就证明了我们的断言。

于是可设$b=2c$而得到$\left(\frac{x_1}{2}\right)^2=ac,(a,c)=1$。由定理4.6就得到

$$a=d^2,c=f^2,d>0,f>0,(d,f)=1$$

再由$x_1^2=2ab,y_1^2=a^2-b^2,z_1=a^2+b^2$即得

$$y_1^2=a^2-b^2=a^2-4c^2=d^4-4f^4$$

或者
$$(2f^2)^2+y_1^2=(d^2)^2$$

现在我们证明,$2f^2$和y_1一定是互素的。假若不然,则必存在素数p使得$p\mid 2f^2$,$p\mid y_1$,由$c=f^2,b=2c$推出$p\mid c,p\mid b$。因而$p\mid b,p\mid y_1$,再由$y_1^2=a^2-b^2$推出$p\mid a$,由$p\mid a,p\mid b$就得出$(a,b)>p>1$,但这与$(a,b)=1$矛盾,所得的矛盾就说明必然成立$(2f^2,y_1)=1$。

于是再由定理3.5.3即得

$$2f^2=2lm,d^2=l^2+m^2,l>0,m>0,(l,m)=1$$

由此又得出

$$f^2=lm,l>0,m>0,(l,m)=1$$

于是再由定理3.4.6即得

$$l=r^2,m=s^2,r>0,s>0,(r,s)=1$$

代入$d^2=l^2+m^2$中即得

$$r^4+s^4=d^2,r>0,s>0,(r,s)=1$$

这就是说,从假定方程$x^4+y^4=z^2$有一组正整数解$x_1>0,y_1>0,z_1>0$出发,我们就又可以得出另一组正整数解$x_2=r>0,y_2=s>0,z_2=d>0$。但是这两组解是不一样的,区别就在于z_1和z_2的大小不一样。实际上$z_2=d\leqslant d^2=a<a^2+b^2=z_1$,于是再从方程$x^4+y^4=z^2$正整数解$x_2>0,y_2>0$,$z_2>0$出发,用与上面完全一样的推理又可得出方程$x^4+y^4=z^2$另一组正整数

解 $x_3>0, y_3>0, z_3>0$,如此反复进行,乃至无穷,就可得到方程 $x^4+y^4=z^2$ 的无穷组正整数解和一窜无穷的,严格递减的数列

$$z_1 > z_2 > \cdots > z_n > \cdots >$$

但由于 z_1 是一个有限的正整数,根据整数的性质法则 3.1.4 可知,上述数列中只可能有有限项,这就得出矛盾,所得的矛盾说明方程 $x^4+y^4=z^2$ 不可能存在任何正整数解。

以上证明定理的方法就称为无穷递降法,在这个例子中,它其实就是反复应用定理 3.5.3 和定理 3.4.6。它也可以写成另一种形式,即一开始假定方程 $x^4+y^4=z^2$ 存在正整数解后,根据自然数的最小数原理可知,在这些解中,必存在着一组使得 z 最小的解 $x_1>0, y_1>0, z_1>0$。然后从这组解的存在出发,用和上面同样的推理可以得出方程 $x^4+y^4=z^2$ 存在另一组正整数解 $x_2>0$, $y_2>0, z_2>0$ 并且 $z_1>z_2$,而这与 z_1 的最小性矛盾。

从定理 3.5.4 显然就可得出下面的定理。

定理 3.5.5　方程 $x^4+y^4=z^4$ 不存在正整数解。

读者一定注意到我们没有证明 $n=3$ 时的费马问题及直接从 $n=2$ 跳到 $n=4$ 的情况。实际上 $n=3$ 的情况反而比 $n=4$ 的情况复杂(至少,作者本人不知道其他更简单的证明方法),要想知道如何解决 $n=3$ 的费马问题,在本书的体系中,必须要等到看完了下一节之后。用一句旧小说中的套话来说就是欲知后事如何,且听下回分解。

习题 3.5

1. 把 100 个苹果分成两堆,使得一堆是 7 的倍数,另一堆是 11 的倍数。

2. 把 $\frac{23}{30}$ 和 $\frac{17}{60}$ 写成两两互素的三个既约分数之和。

3. 有面值 1 元、2 元和 5 元的人民币共 50 张,他们的总值是 80 元,问这些面值的人民币各多少张?

4. 设 $(a,b)=1, a>0, b>0$。证明:所有大于 $ab-a-b$ 的整数一定可以表示成为 $ax+by(x\geqslant 0, y\geqslant 0)$ 的形式,但是 $ab-a-b$ 不能表示成为这种形式。

5. 设 a, b, c 是两两互素的正整数。证明:所有大于 $2abc-ab-bc-ac$ 的整数一定可以表示成为 $xbc+yca+zab(x\geqslant 0, y\geqslant 0, z\geqslant 0)$ 的形式,但是 $2abc-ab-bc-ac$ 不能表示成为这种形式。

6. 设一个直角三角形的三条边都是整数,证明:

(1) 它的面积不可能等于它的斜边的长度;

(2) 它的面积不可能是一个完全平方数。

7. 设一个直角三角形的两个直角边都是整数，证明它的两个直角边的乘积必可被 12 整除。

8. 设一个直角三角形的三条边都是整数，证明它的三条边的乘积必可被 60 整除。

9. 证明：等式 $n^2 + (n+1)^2 = 2m^2$ 不可能成立，其中 m, n 都是自然数。

10. (1) 验证：$3^2 + 4^2 = 5^2, 20^2 + 21^2 = 29^2, 119^2 + 120^2 = 169^2$；

(2) 证明：如果

$$a^2 + (a+1)^2 = c^2$$

则
$$(3a + 2c + 1)^2 + (3a + 2c + 2)^2 = (4a + 3c + 2)^2$$

你是否能给出一个类似的公式？

(3) 设 $a^2 + (a+1)^2 = c^2$，且 $u = c - a - 1, v = \dfrac{2a - c + 1}{2}$，证明 v 必是一个整数，并且 u, v 必满足关系式

$$\frac{u(u+1)}{2} = v^2$$

11. 求出不定方程 $x^2 + 3y^2 = z^2, (x, y) = 1$ 的所有正整数解。

12. 证明：不定方程 $x^4 + 4y^4 = z^2, x > 0, y > 0$ 不存在整数解。

13. 证明：不定方程 $x^4 - y^4 = z^2, y > 0, z > 0$ 不存在整数解。

14. 证明：两个相邻的自然数的乘积不可能是一个整数的方幂。

15. 证明：三个相邻的自然数的乘积不可能是一个整数的方幂。

3.6 同余式

大千世界，千奇百态。如果我们不对外界的事物加以正确而合理的分类，恐怕我们的头脑将是一团乱麻，而且永远抓不到问题的本质。

比如说，你碰到一个不认识的字，当然就会想到去查字典，查字典实际上就是把字典中的所有的字按照一定的原则作了分类。最简单的查法是按汉语拼音的字母顺序去查，一般很快就可以查到，然后你就可以知道这个字的含义是什么。但是假如你连这个字的发音都不知道，那就有点费劲了，这时只好用部首查字法，所以这个字典至少要有两套分类法才好用。然而好多人用这个部首查字法去查字感到十分费劲，因为它的分类原则有时和直观相差太远。比如最普通的，你想查“摩”子，这个字很普通，是经常用的，但是好多人按部首查字法就查不着这个字，因为他们都按直观去查“广”，“木”，“手”这些部首，结果都不对，我一开始也查不到这个字，觉得连这么普通的字都查不到，简直太不可思议，后来才知道要去查“麻”字旁，原来这个部首查字法的编者是把“摩”看成是把

"麻"字外面的那个"广"字拉长了的"麻"再加一个"手"字。这个就有点太牵强了,你把"麻"字外面的那个"广"字拉长了就不是"麻"了嘛。这种例子还有很多,所以他还专门弄了一个难字表,表示连他自己都知道按他这个办法,有好多字不好分类。不过有了计算机后,我可以告诉你一个小诀窍,不用这么费劲了。这个诀窍如下:

(1) 打开 word 2003,在屏幕下方的输入法菜单条中调出微软拼音输入法2003;

(2) 单击微软拼音输入法 2003 菜单条中的"输入板"图标(右数第二个图标);

(3) 单击"输入板"中的"清除",将输入板中现有的笔记清除;

(4) 用鼠标在"输入板"左边的空白框中写上你想查的字,例如"爿"字;这时"输入板"左边的框中就会出现你写的字"爿"单击这个字,即可把这个字输入到 word 中;

(5) 拖动鼠标选中你所输入的字"爿"(即使它变黑);

(6) 单击 word 上面的菜单条中的格式 → 中文版式 → 拼音指南,就会出现一个对话框,里面有"爿"字的拼音(念"盘")。

但有时这个办法也不灵,比如你按上面的办法写上"枬"字(好些人错把这个字读成"丹"),或者"踅"字,"输入板"左边的框中就找不到你写的字。这时你可试用下面的方法:

(1) 打开 word,在 word 中输入你想查的字的一个部分,例如对"枬"字你可试用"木"字或"丹"字,对"踅"字你可试用"折"字或"足"字;(如果这一部分并不是一个单个的字,而是一个偏旁,你可打开全拼输入法,用拼音输入法输入 pianpang 即可出现各种偏旁的符号)

(2) 选中你所输入的字或偏旁(这个字指你想要查的那个字的一部分,即上面所举的"木","丹","折"或"足"字);

(3) 单击 word 上面的菜单条中的插入 → 符号,这时就会出现一个对话框,在此对话框中,word 已经自动定位到你所输入的偏旁符号上,在这个符号附近(如当前出现的字中没有你要查的字,可下拉左边的滑块查看全部(即单击左面的竖直菜单条下方的向下箭头),例如输入"木"之后,按照上面所说的方法,在当前出现的字符中,没有"枬"这个字,这时盯住对话框的最底下一行,单击向下箭头 6 次后,在最底下一行的从左数第 3 个字就是"枬"字。找到你要查的字后,单击此字,将其选中;然后单击插入 → 关闭,即可把此字输入到 word 中;

(4) 在 word 中选定你刚才输入的字,按 Ctrl + C 将其复制;

(5) 把输入法切换到全拼输入法,用右键单击全拼输入法最左边的图标,选"手工造词",在"词语"文本框中按 Ctrl + v 把"枬"字粘帖上,再随便输入一

个汉字,"外码"窗口中就会出现"枬"(念"然")字的拼音了。

再比如大的图书馆中收藏的书籍数量是极大的,如果你不知道一本书的大概位置,要去找一本书那就如同大海捞针一样茫然了,这时你可借助图书馆的分类法帮助你,目前国内的图书馆一般都采用"中国图书分类法"或"中国科学院图书分类法"。按照"中国图书分类法",数学类的图书的编号是以 O1 开头的,而按照"中国科学院图书分类法",数学类的图书的编号是以 51 开头的,然后再在这个开头下进行更细的分类,例如"中国科学院图书分类法"数学类的下一级细目为:51.1 古典数学;51.2 初等数学;51.3 数理逻辑与数学基础;51.4 数论、代数与组合理论;51.5 几何、拓扑;51.6 分析;51.7 概率论与数理统计;51.8 计算数学;51.9应用数学。根据这个分类,你就可以按照书架上的编号知道大致要在哪里去找你想要查的书了。

做研究工作,刚入门时最难得的是发现一个适合自己做的具体题目,你要想确定这个题目,就要知道关于这一问题的研究历史和现状。美国有一个杂志叫《美国数学评论》(《American Mathematical Reviews》)就可以帮你完成这个任务,比如,假如你对整数问题的研究感兴趣,你可以查 11 条目下的目录,其中 11A 是初等数论方面的信息,在此条目下,你可查到约两年前有谁写过什么论文,发表在什么杂志上,查近5年或近10年的论文,你就可以大致了解在这方面的研究情况了。

以上所说的可以说是根据事物的特征对事物予以分类。但是分类还有另一方面的作用,即一个好的,抓住了事物本质的分类反过来又可以帮助我们发现或揭露事物的内在特征。我们举一个例子。

例 3.6.1 从一个 8×8 的方格表中剪去左上角和右下角得到一个如图 3.6.1 所示的图形 T。问

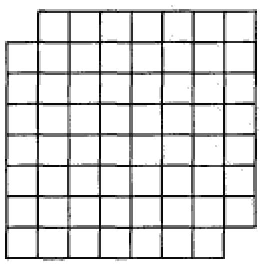


图 3.6.1

(1) 是否能用 30 张 1×2 的小纸片将其不重复也不遗漏地覆盖?

(2) 是否能用 31 张 1×2 的小纸片将其不重复也不遗漏地覆盖?

解 (1) 对第一问稍加思索,就可看出答案是否定的。原因在于图形 T 含

有 62 个小方格，而 30 个 1×2 的小纸片只含有 60 个方格，因此不可能将 T 不重复也不遗漏地覆盖。

这里，我们使用面积对由小方格组成的图形加以分类，面积相同的图形算做一类，那么按照覆盖的定义就可知，能被 30 个 1×2 的小纸片覆盖的图形必须和它属于同一类，即属于面积等于 60 个小方格的类，而图形 T 的面积为 62，不属于这一类，因此不可能被覆盖。这可以说是从定义出发所作的最初级的分类。

(2) 在第二问里，再使用以面积为标准的原则分类就不解决问题了，因为现在在按此原则所作的分类中，图形 T 和 31 张 1×2 的小纸片可以覆盖的图形本来就属于同一类。但是这只是一个必要条件，就是说，要被 31 张 1×2 的小纸片覆盖，方格图形的面积必须是 62，但是反过来面积是 62 的方格图型却不见得就一定能被 31 张 1×2 的小纸片覆盖。经过试验，你可以发现，无论你怎么摆放，使用 31 张 1×2 的小纸片都不可能将图形 T 不重复也不遗漏地覆盖。这就使我们猜测，这一问题的答案也是否定的。但是关键是如何证明这一点。因为人家会说：你没办法盖住，不见得别人没办法盖住。当然你也可以把所有的盖法列举出来，以此证明不存在所说的覆盖，然而这将是极其繁琐的。下面，我们对图形 T 的方格作更细的分类，把 T 中的方格按照国际象棋棋盘的样式，用黑白两种颜色染色，如图 3.6.2。

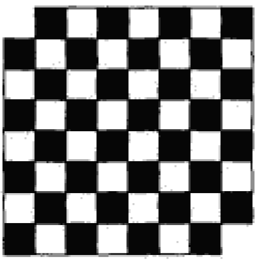


图 3.6.2

把 T 按上述方式染色后，你会发现，一张 1×2 的小纸片无论如何摆放，必然同时盖住一个黑格子和一个白格子，也就是说，能被 31 张 1×2 的小纸片覆盖的图形，不但面积首先得是 62 个格子，而且它的黑格子的数目还必须和白格子的数目相等。而图形 T 被剪掉的两个格子都是白色的，因此 T 的黑格子数目和白格子数目不可能相等(确切地说，T 共有 32 个黑格子和 30 个白格子)。故无论怎么摆放，都不可能用 31 张 1×2 的小纸片将图形 T 不重复也不遗漏地覆盖。这里，我们对图形所作的分类就暴露了用 1×2 的小纸片覆盖一个格子图形时的特性：它同时盖住一个黑格子和一个白格子。

从上面的问题可以看出，为了暴露覆盖的特性，所作的分类是要依赖于覆

盖的方式的，也就是说，当覆盖的方式变了，分类的方式也可能会改变。下面我们再举一个例子。

例 3.6.2 问一个 8×8 的棋盘能否用图 3.6.3 所示的 15 个 L 形纸片和一个田字形纸片不重复也不遗漏地覆盖？



图 3.6.3

解 这回如果你仍然使用例 3.6.1(2) 中的染色方法将什么问题也看不出来。所以这次我们用另一种方法将棋盘染色，如图 3.6.4 所示。

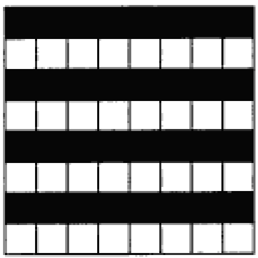


图 3.6.4

这下你可很容易地看出，那个田字形的纸片每次总是盖住 2 个黑格子，2 个白格子，而那个 L 形纸片则盖住 3 个白格子 1 个黑格子或者 3 个黑格子，1 个白格子，总之是每次都盖住奇数个白格子和奇数个黑格子。一旦看出这一点，你就可以进一步进行推理了。

如果所说的覆盖是可能的，那么可设 15 个 L 形纸片各盖住了 $a_1,a_2,\cdots,a_{15}$ 个白格子，$b_1,b_2,\cdots,b_{15}$ 个黑格子，于是棋盘上就应有 $a_1+a_2+\cdots+a_{15}+2$ 个白格子和 $b_1+b_2+\cdots+b_{15}+2$ 个黑格子。

即棋盘上的白格子的数目和黑格子的数目都应该是奇数，但是这正与事实相反。所以无论怎么摆放 L 形纸片和田字形纸片，所说的覆盖都是不可能的。这种染色方法之所以在这种情况下起作用，原因就在于它暴露了 L 形纸片和田字形纸片覆盖图形时的本质区别。

例 3.6.3 从 8×8 的棋盘中剪去左上角之方格，证明：剩余部分不可能存在 3×1 覆盖。

证明 如图 3.6.5，把 8×8 棋盘用以下方式分成 3 类（分别称为 1 色格，2 色格和 3 色格），则共有 1 色格 21 个，2 色格 21 个，3 色格 21 个。剪掉左上角后还剩 20 个 1 色格。而每个 3×1 条无论怎么放置都恰盖住 1，2，3 色格各一个，如果

能够覆盖则共需 21 个 3×1 条，恰盖住 1,2,3 色格各 21 个，现在只有 20 个 1 色格，因此不可能存在所说的覆盖。

1	2	3	1	2	3	1	2
2	3	1	2	3	1	2	3
3	1	2	3	1	2	3	1
1	2	3	1	2	3	1	2
2	3	1	2	3	1	2	3
3	1	2	3	1	2	3	1
1	2	3	1	2	3	1	2
2	3	1	2	3	1	2	3

图 3.6.5

既然可以给图形分类，那么能不能给数字分类呢?当然能，而且一样可以得到出人意料的应用。

回忆我们在 3.5 中证明引理 3.5.5 时用过的一个断言，即 $4n+2$ 形的数不可能是一个完全平方。这个断言如果要想用验证的方式来证明，则由于自然数有无穷多个而不可能执行。但是我们只用了几句话就把它证明了，这是怎么回事呢?原来我们的方法是把全体整数分成奇数和偶数两大类。这样就只须对这两类数来验证这个命题就可以了。也就是说，通过分类，我们把无限转化为有限了。但是有的人又会问，那奇数和偶数不是还是无限多吗，怎么这回就可以验证了呢?不错，分完类后，我们仍然面对无限多的数，但是此无限这回不同于彼无限了，因为奇数和偶数都是有特性的数，如果不分类，他们混在一起，就什么特性也看不出来，分类后，虽然还有无限多个数，但是利用了他们的特性，我们就不需要一个一个地去验证了。所以说有时一个特性要顶无限多个数。

现在我们要问，这种分类方法能不能推广呢?回答是，当然能。这就要退回去看一看奇数和偶数是如何定义的。这个我们都知道。比如有人会说，偶数就是被 2 除得尽的数，奇数就是被 2 除不尽的数。不错，用这种定义，的确可以把这种分类方式推广。比如说，我们可以把被 3 除得尽的数定义为 3 尽数，把被 3 除不尽的数定义为 3 不尽数(或者随便其他什么名称都可以)，但是这种分类太粗，应用意义不大。所以还要再退回去弄清奇数和偶数的确切含义。

由带余数除法，我们知道任何一个数，被 2 去除，余数只可能是 0 或 1，而所谓偶数就是被 2 除余 0 的数，奇数就是被 2 除余 1 的数。这就对头了，这就追到问题的老根子上了。用余数的观点，我们就可以把偶数、奇数的分类方法加以推广了。比如说，我们选定整数 3，那么我们就可以把全体整数分成 3 类：被 3 除余数是 0 的数，被 3 除余数是 1 的数和被 3 除余数是 2 的数。这种分类方法，先要取定一个数作标准，上面的分类中 3 就是这个标准，这个作为标准的数称为“模”，我

们不得不赞叹最先使用这个术语的中国数学家。因为它既是这个词的英语对应词汇“module”的音译，而本身又含有这个字的中文含义。因为如果你去查字典，这个字的第一个含义就是“可作为依据的法式或标准”，对应的词汇有模型、模式、模具、模子、模范、模特，无一不是从原始的标准这个含义发展而来。所以这个词翻译得是“音”，“义”俱得，真是韵味十足，值得品味。

把上面这种分类方法一般化，我们就得到以下的定义：

定义 3.6.1 给定任意一个大于1的自然数 m，称为“模”，我们可以把全体整数以模 m 为标准分成 m 类，即被 m 除余数为 0 的数，即被 m 除余数为 1 的数，…，即被 m 除余数为 $m-1$ 的数，称为模 m 的同余类，分别记为 $\{0\}$，$\{1\}$，…，$\{m-1\}$ $(\bmod m)$（这里的“mod m”读作“模 m”。）

在上面的定义中，我们用 $\{0\}$，$\{1\}$，…，$\{m-1\}$ 来代表 m 的同余类，大括号中的数字是这个同余类被 m 除所得的余数，其实我们可以用这个同余类中的任何一个数来代表这个同余类。为了从形式上表示出这个意思，我们规定：

定义 3.6.2 对任何整数 $q, r, 0 \leqslant r < m$，符号 $\{qm+r\}$ 的意义和 $\{r\}$ 相同，即规定

$$\{qm+r\} = \{r\}$$

由同余类的定义立刻得出：

定理 3.6.1 给定模 m，那么

(1) 模 m 的同余类恰有 m 个；

(2) 设 A 与 B 是模 m 的任意两个同余类，则或者 $A = B$，或者 $A \cap B = \varnothing$；

(3) 任意一个整数 a 必属于 m 的某一个同余类。

我们再定义两个整数集合的下列两种运算的意义：

定义 3.6.3 设 A, B 是两个整数组成的集合，则令

$$A + B = \{a + b \mid a \in A, b \in B\}$$
$$A - B = \{a - b \mid a \in A, b \in B\}$$
$$A \times B = \{ab \mid a \in A, b \in B\}$$

于是我们有：

定理 3.6.2 设 λ 和 μ 是任意整数，则

(1) $\lambda\{a\} + \mu\{b\} \subset \{\lambda a + \mu b\}$；

(2) $\{a\} \times \{b\} \subset \{ab\}$。

证明 (1) 任取 $x \in \lambda\{a\} + \mu\{b\}$ 则由 $\lambda\{a\} + \mu\{b\}$ 的定义知存在着 $u \in \{a\}, v \in \{b\}$，使得 $x = \lambda u + \mu v$。又由 $\{a\}, \{b\}$ 的定义知 $\mu = q_1 m + a$，$v = q_2 m + b$。又设 $\lambda a + \mu b = qm + r, 0 \leqslant r < m$，则

$$x = \lambda u + \mu v = \lambda(q_1 m + a) + \mu(q_2 m + b) = (\lambda q_1 + \mu q_2 + q)m + r$$

因此 $x \in \{r\} = \{qm + r\} = \{\lambda a + \mu b\}$，再由 x 的任意性就得出 $\lambda\{a\} + \mu\{b\} \subset$

$\{\lambda a+\mu b\}$。

(2) 任取 $x\in\{a\}\times\{b\}$，则由 $\{a\}\times\{b\}$ 的定义知存在着 $u\in\{a\}$，$v\in\{b\}$，使得 $x=uv$。又由 $\{a\}$，$\{b\}$ 的定义知 $u=q_1m+a$，$v=q_2m+b$。又设 $ab=qm+r$，$0\leqslant r<m$，则

$$x=uv=(q_1m+a)(q_2m+b)=(q_1q_2m+q_1b+q_2a+q)m+r$$

因此 $x\in\{r\}=\{qm+r\}=\{ab\}$，再由 x 的任意性就得出 $\{a\}\times\{b\}\subset\{ab\}$。

由以上这个定理我们可知，对两个同余类中的整数经过加、减和相乘之后得出来的数所属的同余类是受到一定限制的，这就曝露了有些特殊数的特点。而且由于同余类的数目是有限的，因此我们可以造出表来列举出全部的可能性。

例 3.6.4 列举出一个整数的平方在模 4 下可能属于哪些同余类。

解 由 $0^2=0$，$1^2=1$，$2^2=4=4\cdot1+0$，$3^2=9=2\cdot4+1$ 和定理3.6.2可知

$$x^2\in\{0\}\cup\{1\}\pmod 4$$

也就是说，任何一个整数的平方在模 4 下，只可能属于同余类 $\{0\}$ 或 $\{1\}$，而不可能属于同余类 $\{2\}$ 或 $\{3\}$。我们在 3.5 中证明引理 3.5.5 时就利用了这个结果去证明 $4n+2$ 形的数不可能是一个完全平方。

例 3.6.5 考察两个整数的平方和在模 4 下可能属于哪些同余类。三个整数的平方和在模 8 下可能属于哪些同余类。

解 我们构造图 3.6.6，图中的行和列分别表示我们所取得两个数的同余类，而表中的数表示它们的平方和所属于的同余类。

	0	1	2	3
0	0	1	0	1
1	1	2	1	2
2	0	1	0	1
3	1	2	1	2

图 3.6.6

由图 3.6.6 可以看出 $x^2+y^2\in\{0\}\cup\{1\}\cup\{2\}\pmod 4$，即两个整数的平方和在模 4 下，只可能属于同余类 $\{0\}$，$\{1\}$ 或 $\{2\}$，而不可能属于同余类 $\{3\}$。

类似地，我们可以得出 $x^2+y^2+z^2\in\{0\}\cup\{1\}\cup\{2\}\cup\{3\}\cup\{4\}\cup\{5\}\cup\{6\}\pmod 8$，即三个整数的平方和在模 8 下，只可能属于同余类 $\{0\}$，$\{1\}$，$\{2\}$，$\{3\}$，$\{4\}$，$\{5\}$ 或 $\{6\}$，而不可能属于同余类 $\{7\}$。

例 3.6.6 证明任何奇数的平方必属于 $\{1\}\pmod 8$。

证明 设 x 是一个奇数，则 $x=2n-1$，其中 n 是某一整数，于是

$$x^2=(2n-1)^2=4n(n-1)+1$$

由于 $n-1$ 和 n 这两个连续整数中必有一个是偶数，因此

$$n(n-1)=2k,x^2=4\cdot2k+1=8k+1$$

故 $x^2\in\{1\}\pmod 8$。

例 3.6.7 证明：$x^2+y^2=1\,995$不存在整数解。

证明 由$1\,995\in\{3\}(\bmod 4)$和例3.6.5即得。

例 3.6.8 证明：111…1不可能是一个完全平方数。

证明 由于111…1是一个奇数，由例3.6.6知，只要证明它不属于$\{1\}(\bmod 8)$即可。但是有的人可能会发出感叹，那你不知道111…1中有多少个1，你怎么去除呢？那好吧，我再悄悄地告诉你一个小秘密，你只要去看这个数的末三位数被8除余几就够了。因为111…000是一个被8除余零的数，所以这个数里千位以上的数全是多余，根本不用理它。而$111=8\cdot 13+7$，所以$111\cdots 1\in\{7\}(\bmod 8)$。这就证明了结论。

上面我们对同余类的讨论，虽然已经可以解决许多问题，但是你会体会到，把同余类的结论用下面所说的另一种形式表达，经常会更加方便，甚至是不可替代。

定义 3.6.3 给定模m，如果整数a,b都属于m的同一个同余类，则称a和b在模m下同余，记为$a\equiv b(\bmod m)$（读作"a同余于b模m"）。

我们有

定理 3.6.3 以下三个命题互相等价

(1) $a\equiv b(\bmod m)$；

(2) $a=qm+b$；

(3) $m\mid(a-b)$。

证明 (1)⇒(2)。设$a\equiv b(\bmod m)$，那么按照同余的定义，a,b都属于模m的同一个同余类，不妨设$a\in\{r\}(\bmod m)$，$b\in\{r\}(\bmod m)$。这就是说$a=q_1m+r$，$b=q_2m+r$，因此

$$a=q_1m+r=q_1m+b-q_2m=(q_1-q_2)m+b$$

(2)⇒(3)。设$a=qm+b$，那么$a-b=qm$，因此$m\mid(a-b)$；

(3)⇒(1)。设$m\mid(a-b)$，那么$a-b=qm$。再设$b=q_1m+r$，于是

$$a=b+qm=(q_1+q)m+r$$

因而$a\in\{r\}(\bmod m)$，$b\in\{r\}(\bmod m)$。这就是说a,b都属于模m的同一个同余类，故$a\equiv b(\bmod m)$。

以后在模是什么非常明确而不至于引起误会和混淆的情况下，我们经常把$a\equiv b(\bmod m)$简记为$a\equiv b$。

由定理3.6.3易证以下的同余式的性质：

定理 3.6.4 设同余式的模是m，那么关于模m的同余式有以下性质：

(1) 自反性：$a\equiv a$；

(2) 对称性：如果$a\equiv b$，那么$b\equiv a$；

(3) 传递性：如果$a\equiv b$，$b\equiv c$，那么$a\equiv c$；

(4) 如果 $a \equiv b$，k 是一个整数，那么 $ka \equiv kb$；

(5) 如果 $a_1 \equiv b_1, a^2 \equiv b_2$，那么 $a_1 + b_1 \equiv a_2 + b_2$；

(6) 如果 $a_1 \equiv b_1, a_2 \equiv b_2$，那么 $a_1 - b_2 \equiv a_2 - b_2$；

(7) 如果 $a_1 \equiv b_1, a_2 \equiv b_2$，那么 $a_1 b_1 \equiv a_2 b_2$；

(8) 消去法则：如果 $ac \equiv bc$，且 $(c, m) = 1$，那么 $a \equiv b$；

(9) 如果 $a \equiv b \pmod{m_1}$，$a \equiv b \pmod{m_2}$，$(m_1, m_2) = 1$，则 $a \equiv b \pmod{m_1 m_2}$；

(10) 如果 $x \equiv a$，而 $f(x)$ 是一个整系数多项式，那么 $f(x) \equiv f(a)$；

(11) 如果 $a \equiv b \pmod{m}$，k 是一个正整数，则 $ka \equiv kb \pmod{km}$；

(12) 如果 $a \equiv b \pmod{m}$，d 是 a, b, m 的公因数，则 $\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{d}}$。

证明　我们只证明(8)，(9)，(12) 三条，其余性质的证明请读者自己作为练习。

(8) 如果 $ac \equiv bc$，那么由定理 3.6.3 可知

$$m \mid (ac - bc) = c(a - b)$$

但是由于 $(c, m) = 1$，故由定理 3.3.8 得 $m \mid (a(b)$，因此再由定理 3.6.3 可知 $a \equiv b$。

(9) 如果 $a \equiv b \pmod{m_1}$，$a \equiv b \pmod{m_2}$，那么由定理 3.6.3 可知 $m_1 \mid (a - b)$，$m_2 \mid (a - b)$。但是由于 $(m_1, m_2) = 1$，故由定理 3.3.9 得 $m_1 m_2 \mid (a - b)$，因此再由定理 3.6.3 可知 $a \equiv b \pmod{m_1 m_2}$。

(12) 由 $a \equiv b \pmod{m}$ 和同余式的等价定理(定理 3.6.3)知 $a = b + qm$，在此式两边同除以 d 即得

$$\frac{a}{d} = \frac{b}{d} + q\frac{m}{d}$$

再由同余式的等价定理即知这就是

$$\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{d}}$$

例 3.6.9　求 $437 \times 309 \times 1\,993$ 除以 7 所得的余数。

解　由于 $437 \equiv 3 \pmod 7$，$309 \equiv 1 \pmod 7$，$1\,993 \equiv 5 \pmod 7$，所以

$$437 \times 309 \times 1\,993 \equiv 3 \times 1 \times 5 \pmod 7 \equiv 1 \pmod 7$$

即 $437 \times 309 \times 1\,993$ 除以 7 所得的余数为 1。

例 3.6.10　已知 a 除以 5 余 1，b 除以 5 余 4，问 $3a - b$ 除以 5 余几？

解　由已知条件有 $a \equiv 1 \pmod 5$，$b \equiv 4 \pmod 5$，故

$$3a - b \equiv 3 \times 1 - 4 \pmod 5 \equiv -1 \pmod 5 \equiv 4 \pmod 5$$

即 $3a - b$ 除以 5 余 4。

例 3.6.11　求 11…1(共有 1 993 个 1) 被 7 除所得的余数。

解 研究问题总要先试验一下，实验的目的是看看那种形如11…1的数被7除所得的余数简单，所谓简单，从同余式的观点来看，可以认为0，1，-1都是比较简单的余数。通过6次试验，我们发现 $111\ 111\equiv 0 \pmod 7$，下面我们再看看11…1(共有1 993个1)中共可排列出多少个111 111。由于111 111是6位数，所以只要拿1 993去除以6，看商是多少即可。实际上 $1\ 993=332\times 6+1$。所以我们可以把11…1(共有1 993个1)分成333段，其中最后一段就是1，前面332段每段都是111 111。即

$$
\begin{aligned}
11\cdots 1(\text{共有 }1\ 993\text{ 个 }1) &= (111\ 111)\cdots(111\ 111)1(\text{共有 }332\text{ 个括弧}) = \\
&(111\ 111)\cdots(111\ 111)0+1\equiv \\
&0+1 \pmod 7\equiv 1 \pmod 7
\end{aligned}
$$

故11…1(共有1 993个1)被7除所得的余数为1。

这道题也可以用另一种方法作，但也不能避免实验。

11…1(共有1 993个1) $=1+10+10^2+\cdots+10^{1\ 992}$，下面就是要试验对什么 n 能有 $10^n\equiv 1 \pmod 7$。我们有

$$
\begin{aligned}
&1\equiv 1\\
&10\equiv 3\\
&10^2\equiv 10\times 10\equiv 10\times 3\equiv 2\\
&10^3\equiv 10\times 2\equiv 6\\
&10^4\equiv 10\times 6\equiv 4\\
&10^5\equiv 10\times 4\equiv 5\\
&10^6\equiv 10\times 5\equiv 1\\
&\vdots\\
&10^{1\ 992}=10^{6\times 332}=(10^6)^{332}\equiv 1^{332}\equiv 1
\end{aligned}
$$

所以

$$
\begin{aligned}
&11\cdots 1(\text{共有 }1\ 993\text{ 个 }1)=1+10+10^2+\cdots+10^{1\ 992}\equiv\\
&(1+3+2+6+4+5)+(1+3+2+6+4+5)+\cdots+(1+3+2+6+4+\\
&5)+1(\text{共有 }332\text{ 个括弧})\equiv\\
&0+0+0+\cdots+1(\text{共有 }332\text{ 个 }0)\equiv 1
\end{aligned}
$$

例 3.6.12 70个数排成一排，除两头的数外，中间每个数的3倍都等于它两边的数之和，从左边数起，开头的几个数为

$$0,1,3,8,21,\cdots$$

问第70个数(也就是这排数最右边的数)被6除的余数。

解 根据题目已给的条件，这70个数原则上都可以用递推公式

$$a_{n+2}=3a_{n+1}-a_n, a_1=0, a_2=1$$

逐步求出，所以只要给定开头两个数，这70个数就都被确定了。求出第70个数

后，再用 6 去除它，就可求出所需的余数了。这虽然给出一个解决问题的方案，但是工作量太大。能不能有工作量较小的方案呢？

由于题目并不要求我们求出第 70 个数，而只要求求出它被 6 除所得的余数，因此我们的思路转向直接去求出余数。方法是再造一个数列，使得新数列的每一项和原数列的对应项在模 6 下同余。设新数列的通项是 $b_n \equiv a_n \pmod 6$，那么根据 a_n 的递推公式就可得出 b_n 的递推公式

$$b_{n+2} \equiv 3b_{n+1} - b_n \pmod 6$$

至于新数列的前两项，我们可以取得跟原数列相同，即取 $b_1 = 0, b_2 = 1$。那有人会问，你这个新数列不是还得靠递推一项一项地算下去吗？那你造这个新数列有什么意义呢？初一看起来，两个数列的构成规律完全相同，但是再仔细研究一下，就会发现它们的差别在于新数列是关于模 6 同余的，这就使得新数列与原数列在性质上有了两个本质的差别。第一个差别是新数列是有界的（每一项都不超过 6），这个性质再加上数列的递推性就得出第二个差别，就新数列必然是周期数列。我们可以逐步算出新数列的前几项，直到连续出现两个相同项为止。下面是计算的结果

$$0,1,3,2,3,1,0,5,3,4,3,5,0,1,\cdots$$

由此看出新数列的周期是 12。由于 $70 = 5 \times 12 + 10$，因此原数列的 70 项被 6 除所得的余数与上面的数列中的 10 项相同，即所求的余数是 4。

例 3.6.13　求 $1^4 + 2^4 + \cdots + 1\,993^4$ 的个位数字。

解　这道题一开始的工作还是试验，我们计算以下各数关于模 10 的余数：

$$1^4 \equiv 1$$
$$2^4 \equiv 16 \equiv 6$$
$$3^4 \equiv 81 \equiv 1$$
$$4^4 \equiv 256 \equiv 6$$
$$5^4 \equiv 625 \equiv 5$$
$$6^2 \equiv 6, 6^3 \equiv 6, 6^4 \equiv 6$$
$$7^2 \equiv 9, 7^3 \equiv 3, 7^4 \equiv 1$$
$$8^2 \equiv 4, 8^3 \equiv 2, 8^4 \equiv 6$$
$$9^2 \equiv 1, 9^3 \equiv 9, 9^4 \equiv 1$$
$$10^4 \equiv 0$$

因此

$$\begin{aligned}1^4 + 2^4 + \cdots + 1\,993^4 &= (1^4 + 2^4 + \cdots + 10^4) + \cdots + (1^4 + 2^4 + \cdots + 10^4) + 1^4 + \\ &\quad 2^4 + 3^4\text{（共有 199 个括弧）} \equiv \\ &\quad 199 \times (1 + 6 + 1 + 6 + 5 + 6 + 1 + 6 + 1 + 0) + 1 + 6 + \\ &\quad 1 \equiv (-1) \times 3 + 8 \equiv 5\end{aligned}$$

故 $1^4+2^4+\cdots+1\,993^4$ 的个位数字是 5。

例 3.6.14 求证:$74 \mid 75^{378}-1$。

证明 只须证 $75^{378}\equiv 1 \pmod{74}$ 即可。

由于 $75\equiv 1 \pmod{74}$,这就立刻得出 $75^{378}\equiv 1 \pmod{74}$。

例 3.6.15 求 $1\,949^{1\,993}$ 被 7 除所得的余数。

解 首先把上式的底化简,由于 $1\,949\equiv 3 \pmod 7$,故 $1\,949^{1\,993}\equiv 3^{1\,993} \pmod 7$。下面还是试验,由计算得出

$$3\equiv 3$$
$$3^2\equiv 9\equiv 2$$
$$3^3\equiv 27\equiv 6\equiv -1$$

故 $$3^{1\,993}=3^{3\times 664+1}=(3^3)^{664}\cdot 3\equiv(-1)^{664}\cdot 3\equiv 3 \pmod 7$$

例 3.6.16 今天是星期一,问 $47^{35^{23}}$ 天之后是星期几?

解 这道题实际上就是要求 $47^{35^{23}}$ 被 7 除所得的余数。

首先注意 $47^{35^{23}}$ 的含义是 $47^{(35^{23})}$ 而不是 $(47^{35})^{23}$。与上题一样,首先化简底数。我们有 $47\equiv 5 \pmod 7$。以下还是先进行试验,由(对模 7)计算得

$$5^1\equiv 5$$
$$5^2\equiv 25\equiv 4$$
$$5^3\equiv 4\cdot 5\equiv 20\equiv -1$$
$$5^6\equiv (5^3)^2\equiv 1$$

故只须把 35^{23} 写成 $6k+r$ 的形式就好算了,于是又要求 35^{23} 被 6 除所得的余数。这个求法本来应该跟上面一样还是先进行试验,但是这里正好有 $35\equiv -1 \pmod 6$,所以就有

$$35^{23}\equiv(-1)^{23} \pmod 6\equiv -1\equiv 5$$

因此 $35^{23}=6k+5$。而

$$47^{35^{23}}\equiv 5^{35^{23}}\equiv 5^{6k+5}\equiv(5^6)^k\cdot 5^5\equiv 3 \pmod 7$$

也就是说,从今天开始算起的第 $47^{35^{23}}$ 天是星期三,而 $47^{35^{23}}$ 天之后就是星期四。

例 3.6.17 求 $14^{14^{14}}$ 的末两位数。

解 原则上可以用上例的方法去做,但是如果直接取 100 做模,由于模较大,可能要试验 100 多次才能找到一个指数 n 使得 $14^n\equiv 1 \pmod{100}$,所以具体实施起来工作量很大。我们必须找到一个可行的方案。由于 $100=4\times 25$,所以我们可以 4 和 25 作为模先进行计算如下

$$14\equiv 2 \pmod 4$$
$$14^2\equiv 0 \pmod 4$$

$$14 \equiv 14 \pmod{25}$$
$$14^2 \equiv 196 \equiv -4 \pmod{25}$$
$$14^3 \equiv (-4) \cdot 14 \equiv -56 \equiv -6 \pmod{25}$$
$$14^4 \equiv (-6) \cdot 14 \equiv -84 \equiv 16 \pmod{25}$$
$$14^5 \equiv 16 \cdot 14 \equiv 224 \equiv -1 \pmod{25}$$
$$14^{10} \equiv 1 \pmod{25}$$

由于$[2,5]=10$,所以最后我们有$14^{10} \equiv (14^2)^5 \equiv 0 \pmod 4$,$14^{10} \equiv 1 \pmod{25}$。这一结果是为了最后用的。目前为了对最底下的那个 14 应用上述结果,我们需要首先把底 14 的指数 14^{14} 表示成$10k+r$的形式,即求14^{14}被10除所得的余数,也就是求 14^{14} 的个位数。仍采用实验的方法,由计算(对模 10)得到

$$14 \equiv 4, 14^{14} \equiv 4^{14}$$
$$4 \equiv 4$$
$$4^2 \equiv 16 \equiv 6$$
$$4^3 \equiv 6 \cdot 4 \equiv 24 \equiv 4$$
$$\vdots$$
$$4^{14} \equiv 6$$
$$14^{14} \equiv 4^{14} \equiv 6$$

因此$14^{14}=10k+6$,由这个式子和已证的$14^{10} \equiv (14^2)^5 \equiv 0 \pmod 4$,$14^{10} \equiv 1 \pmod{25}$就得到

$$A = 14^{14^{14}} = 14^{10k+6} \equiv (14^2)^{5k+3} \equiv 0 \pmod 4$$
$$A = 14^{14^{14}} = 14^{10k+6} \equiv (14^{10})^k 14^6 \equiv -14 \equiv 11 \pmod{25}$$

也就是说$A \in \{4n \mid n=1,2,3,\cdots\} \cap \{25n+11 \mid n=1,2,3,\cdots\}$,在这个交集里只有 36 不超过 100。因此我们得到$A \equiv 36 \pmod 4$,$A \equiv 36 \pmod{25}$。又由于$(4,25)=1$,故由定理 3.6.4 即得$A \equiv 36 \pmod{4 \cdot 25} \equiv 36 \pmod{100}$。

故$14^{14^{14}}$的末两位数是 36。

例 3.6.18 求$2(x^5+y^5+1)=5xy(x^2+y^2+1)$的所有整数解。

解 (1) 首先注意,原方程的任意一组解不可能都是奇数,否则方程的左边是偶数而方程的右边是奇数,这是不可能的。由x,y的对称性,不妨设x是偶数。

(2) $2(x^5+y^5+1)-5xy(x^2+y^2+1)=(x+y+1)f(x,y)$

其中

$$\begin{aligned} f(x,y) = {} & 2x^4-2x^3y+2x^2y^2-2xy^3+2y^4- \\ & 2x^3-x^2y-xy^2-2y^3+ \\ & 2x^2-xy+2y^2-2x-2y+2= \end{aligned}$$

$$2y^4 - xy^2 - 2y^3 - xy + 2y^2 - 2y + 2 \pmod 4 \equiv$$
$$2y^2(y(y-1)) - xy(y+1) + 2y(y-1) + 2 \pmod 4$$

由于 $y(y-1)$ 和 $y(y+1)$ 都是 2 的倍数，因此 $f(x,y) \equiv 2 \pmod 4$。这就是说，对任意整数 x, y 都有 $f(x,y) \neq 0$。

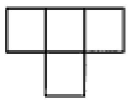
由上面的分解式即知此方程当且仅当 $x+y+1=0$ 时有整数解，因此原方程的整数解为 $y=-x-1$，其中 x 为任意整数。

习题 3.6

1. 给了一个 5×5 的格子纸，从任意一个格子开始顺次填上 1,2,3,…,25 这 25 个数。证明：无论怎么填写，不可能使填着 25 的格子和填着 1 的格子是相邻的。

2. 证明：$x^2 - 4y^2 = 3$ 不存在整数解。

3. 给了一个 8×8 的国际象棋盘，研究是否能用 15 个如下的 T 形纸片



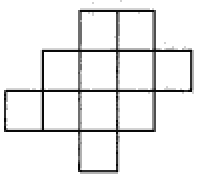
3 题图

和一个 2×2 的田字形字片将其不重复也不遗漏地覆盖？证明你的结论。

4. 证明：在 9×9 的国际象棋盘中，马不可能在遍历每个方格恰一次后回到出发点。

5. 证明：19951995…1995 不可能是一个完全平方数。

6. 证明：如图的残棋盘不可能存在 2×1 的日形块覆盖。



6 题图

7. 对 8×8 棋盘是否存在每个日形块都压住一条横线或纵线的覆盖？

8. 证明：$4\times n$ 国际象棋盘上的马不可能从某一点出发跳遍每格一次又回到出发点。

9. 如果 n 是奇数，证明 $3\times n$ 棋盘不可能存在 3－L 形覆盖。

10. (1) 如果 n 不能被 3 整除，则 $2\times n$ 棋盘不可能用 3－L 块覆盖。

(2) 如果 n 可被 3 整除，则 $2\times n$ 棋盘可以用 3－L 块覆盖。

11. (1) 如果 n 不能被 2 整除，则 $3\times n$ 棋盘不可能用 3－L 块覆盖。

(2) 如果 n 可被 2 整除，则 $3 \times n$ 棋盘可以用 3 - L 块覆盖。

12. 在如下染色的棋盘中

1	2	3	1	2	3	1	2
2	3	1	2	3	1	2	3
3	1	2	3	1	2	3	1
1	2	3	1	2	3	1	2
2	3	1	2	3	1	2	3
3	1	2	3	1	2	3	1
1	2	3	1	2	3	1	2
2	3	1	2	3	1	2	3

12 题图

(1) 如果去掉一个 1 色格，证明：不存在 3×1 覆盖；

(2) 如果去掉一个 3 色格，证明：不存在 3×1 覆盖；

(3) 去掉一个位于 3 行 3 列的 2 色格，证明：剩余部分存在 3×1 覆盖；

(4) 去掉一个位于 1 行 2 列的 2 色格，证明：剩余部分不存在 3×1 覆盖；

13. 能否用一个 3 - L 块和 11 个 3×1 块盖住 6×6 棋盘？

14. 证明：$641 \mid 2^{2^5}$。

15. 设 a 是一个奇数，证明 $a^{2^n} \equiv 1 \pmod{2^{n+2}}$，$n \geqslant 1$。

16. 证明：$A = 2\,222^{5\,555} + 5\,555^{2\,222}$ 和 $B = 3\,333^{4\,444} + 4\,444^{3\,333}$ 都可被 7 整除。

17. 证明：5 个连续的正整数之积不可能是一个完全平方数。

18. 证明：5 个连续的正整数的平方和不可能是一个完全平方数。

19. 设 $n = 4k + 2$，x_i 是 $+1$ 或者 -1，证明：$x_1 + 2x_2 + \cdots + nx_n \neq 0$。

20. 证明：把一个 1 987 位的正整数 $a_1 a_2 \cdots a_{1\,987}$ 的各位数字任意重新排列后所得的新数与原数之和不可能等于 99…9(共有 1 987 个 9)。

21. 证明：100…03(共有 1 989 个 0) 不可能表示成两个整数的平方和。

22. 证明：方程 $x_1^4 + x_2^4 + \cdots + x_{14}^4 = 1\,599$ 没有整数解。

23. 设 $N = 1 \times 3 \times 5 \times 7 \times \cdots \times 1\,983$，求 N 的末三位数。

24. 证明：方程组

$$abcd - a = 1961$$
$$abcd - b = 961$$
$$abcd - c = 61$$
$$abcd - d = 1$$

不存在整数解 a, b, c, d，其中 $abcd$ 表示一个四位数。

25. 把由 1 开始的自然数，依次写下去，一直写到 198 位为止，求这个数被 9

除所得的余数是多少。

26. 证明：$2\ 730 \mid n^{13} - n$。

27. 设 p 为素数，证明：$2^p + 3^p$ 不可能是一个正整数的方幂。

3.7 欧拉定理和费马小定理

我们在3.6中解题时，对题目中给定的一个整数 a 和模m，经常要用实验的方法去求一个指数 k，使得 $a^k \equiv 1 \pmod m$，一旦求得这个指数，以后的计算就可以大为简化。不过这样试验，总让人有碰运气的感觉，起码心里不那么踏实，不知道这个指数什么时候才能试验出来。在这一节里，我们就证明，在一定条件下，这个指数一定存在，而且可以用公式求出来。

首先我们引进一个自然数的函数。

定义3.7.1 设 m 是一个正整数，那么 $\varphi(m)$ 表示 $0,1,2,\cdots,m-1$ 这 m 个数中与 m 互素的整数的个数，称为欧拉函数。

例如，$\varphi(1)=1, \varphi(2)=1, \varphi(3)=2, \varphi(4)=2, \varphi(5)=4, \varphi(6)=2$。

为了得出欧拉函数的一些性质，我们先证明下面的几个定理。

定理3.7.1 设 a 是一个整数$(a,m)=1$，x 遍历 $0,1,2,\cdots,m-1$ 中所有与 m 互素的整数，那么 ax 被m除所得的余数也遍历 $0,1,2,\cdots,m-1$ 中所有与 m 互素的整数，即若$\{r_1,r_2,\cdots,r_{\varphi(m)}\}$ 是小于 m 且与 m 互素的正整数的集合，$\{r'_1,r'_2,\cdots,r'_{\varphi(m)}\}$ 是 $ar_1,ar_2,\cdots,ar_{\varphi(m)}$ 被 m 除所得的余数的集合，那么 $r'_1, r'_2,\cdots,r'_{\varphi(m)}$ 只不过是 $r_1,r_2,\cdots,r_{\varphi(m)}$ 的一个排列，或者

$$\{x \mid (x,k)=1, k=0,1,2,\cdots,m-1\} = \{ax(\mathrm{mod}\ m) \mid (x,k)=1,\\ k=0,1,2,\cdots,m-1\}$$

这里 $ax(\mathrm{mod}\ m)$ 表示 ax 被m除所得的余数。

证明 根据欧拉函数的定义，ax 通过$\varphi(m)$个整数。由于$(a,m)=1$，$(x,m)=1$，故$(ax,m)=1$。这就证明了 ax 通过的$\varphi(m)$个整数都是与 m 互素的。我们只须证明在模 m 下，ax 是两两不同余的，那么由于在模 m 下，所有与 m 互素的非负整数恰有 $\varphi(m)$ 个。于是 ax 在模m 下所通过的整数就只能是 $0,1,2,\cdots,m-1$ 中所有与 m 互素的整数了。

如果 $ax_1 \equiv ax_2 \pmod m$，那么由于$(a,m)=1$，故由同余式的性质知，$x_1 \equiv x_2 \pmod m$，这就证明了 ax 是两两不同余的。

例如，设 $a=4, m=15$。$0,1,2,\cdots,14$中与15互素的数是$1,2,4,7,8,11,13,14$，当 x 遍历这8个数时，$4x$ 遍历$4,8,16,28,32,44,52,56$这8个数。在模15下，这8个数分别同余于$4,8,1,13,2,14,7,11$。还是原来的那8个数，只不过次序变

了而已。

其实在我们上面的证明里，只在证明 ax 与 m 互素时用到了条件 $(a,m)=1$。所以用完全同样的方法(但是去掉 ax 与 m 互素这一要求)，我们可以证明下面的定理。

定理 3.7.2 设 a,b 是两个整数。$(a,m)=1$，那么当 x 遍历 $0,1,2,\cdots,m-1$ 这 m 个数时，$ax+b$ 在模 m 下也遍历 $0,1,2,\cdots,m-1$ 这 m 个数。即

$$\{0,1,2,\cdots,m-1\}=\{ax+b(\mathrm{mod}\ m)\mid x=0,1,2,\cdots,m-1\}$$

或者说 $ax+b$ 被 m 去除所得的余数遍历 $0,1,2,\cdots,m-1$ 这 m 个数(但不一定是按照前面的顺序的)。

下面是两个更复杂的这种类型的定理。

定理 3.7.3 设 m_1,m_2 是两个互素的正整数，c 是一个任意的整数，那么当 x_1,x_2 分别通过集合 $\{0,1,2,\cdots,m_1-1\}$ 以及集合 $\{0,1,2,\cdots,m_2-1\}$ 时，$m_2x_1+m_1x_2+c$ 被 m_1m_2 去除所得的余数就通过集合 $\{0,1,2,\cdots,m_1m_2-1\}$ 中的每个数恰一次。

证明 当 x_1 通过 $0,1,2,\cdots,m_1-1$ 时，m_2x_1 生成 m_1 个数，而当 x_2 通过 $0,1,2,\cdots,m_2-1$ 时，m_1x_2 生成 m_2 个数，因此 m_2x_1 和 m_1x_2 互相搭配恰生成 m_1m_2 个数。生成的每个数再加上 c 仍得到 m_1m_2 个数。我们只要证明这 m_1m_2 个数被 m_1m_2 除所得的余数两两不同即可。

假设存在两个这种类型的数 $m_2x_1+m_1x_2+c$ 和 $m_2y_1+m_1y_2+c$，被 m_1m_2 去除所得的余数是相同的。其中

$$x_1,y_1\in\{0,1,2,\cdots,m_1-1\},x_2,y_2\in\{0,1,2,\cdots,m_2-1\}$$

那么就有

$$m_2x_1+m_1x_2+c\equiv m_2y_1+m_1y_2+c(\mathrm{mod}\ m_1m_2)$$

因此

$$m_1m_2\mid m_2(x_1-y_1)+m_1(x_2-y_2)$$

而由于 $m_1\mid m_1m_2,m_2\mid m_1m_2$，我们就得出

$$m_1\mid m_2(x_1-y_1)+m_1(x_2-y_2)$$

和

$$m_2\mid m_2(x_1-y_1)+m_1(x_2-y_2)$$

再从 $m_1\mid m_1(x_2-y_2)$ 和 $m_2\mid m_2(x_1-y_1)$ 这两式进一步得出 $m_1\mid m_2(x_1-y_1)$ 和 $m_2\mid m_1(x_2-y_2)$。

由于 $(m_1,m_2)=1$，因此由上面两个式子就得出 $m_1\mid|x_1-y_1|,m_2\mid|x_2-y_2|$。而由于

$$x_1,y_1\in\{0,1,2,\cdots,m_1-1\},x_2,y_2\in\{0,1,2,\cdots,m_2-1\}$$

故由这两个式子就得出

$$m_1\leqslant|x_1-y_1|<m_1,m_2\leqslant|x_2-y_2|<m_2$$

这显然是一个矛盾，所得的矛盾就表明不可能存在两个形如 $m_2x_1+m_1x_2+c$ 和 $m_2y_1+m_1y_2+c$ 的数使得它们被 m_1m_2 去除所得的余数是相同的。这也就是说 $m_2x_1+m_1x_2+c$ 被 m_1m_2 去除所得的余数通过集合 $\{0,1,2,\cdots,m_1m_2-1\}$ 中的每个数恰一次。

例如，当 $m_1=3,m_2=5$ 时，$\{0,1,2,\cdots,m_1-1\}=\{0,1,2\}$，$\{0,1,2,\cdots,m_2-1\}=\{0,1,2,3,4\}$。

$$
\begin{aligned}
m_2x_1+m_1x_2=&\{5\cdot 0+3\cdot 0,5\cdot 1+3\cdot 0,5\cdot 2+3\cdot 0\},\\
&\{5\cdot 0+3\cdot 1,5\cdot 1+3\cdot 1,5\cdot 2+3\cdot 1\},\\
&\{5\cdot 0+3\cdot 2,5\cdot 1+3\cdot 2,5\cdot 2+3\cdot 2\},\\
&\{5\cdot 0+3\cdot 3,5\cdot 1+3\cdot 3,5\cdot 2+3\cdot 3\},\\
&\{5\cdot 0+3\cdot 4,5\cdot 1+3\cdot 4,5\cdot 2+3\cdot 4\}=\\
&\{0,5,10,3,8,13,6,11,16,9,14,19,12,17,22\}
\end{aligned}
$$

这个集合中的数被 $m_1m_2=15$ 去除所得的余数的集合为

$$
\begin{aligned}
&\{0,5,10,3,8,13,6,11,1,9,14,4,12,2,7]=\\
&\{0,1,2,3,4,5,6,7,8,9,10,11,12,13,14\}
\end{aligned}
$$

$m_2x_1+m_1x_2$ 正好不多不少遍历了集合 $\{0,1,2,\cdots,m_1m_2-1\}$ 中每个元素一遍。

定理 3.7.4 设 m_1,m_2 是两个互素的正整数，那么当 x_1 遍历 $0,1,2,\cdots,m_1-1$ 中所有 m_1 与互素的数，x_2 遍历 $0,1,2,\cdots,m_2-1$ 中所有与 m_2 互素的数时，$m_2x_1+m_1x_2$ 被 m_1m_2 去除所得的余数就遍历 $0,1,2,\cdots,m_1m_2-1$ 中所有与 m_1m_2 互素的数。

证明 由定理 3.7.3 已证明的结论我们知道在定理的条件下形如 $m_2x_1+m_1x_2$ 的数都是互不同余的，因此我们只须证明 $m_2x_1+m_1x_2$ 被 m_1m_2 去除所得的余数都是与 m_1m_2 互素的，并且反过来 $0,1,2,\cdots,m_1m_2-1$ 中所有与 m_1m_2 互素的数都与一个形如 $m_2x_1+m_1x_2$ 的数同余即可。

(1) 设 $m_2x_1+m_1x_2=qm_1m_2+r,0\leqslant r<m_1m_2$。如果 r 与 m_1m_2 不是互素的，那么必存在一个素数 p 使得 $p\mid(r,m_1m_2)$，即 $p\mid r,p\mid m_1m_2$。因此 $p\mid(m_2x_1+m_1x_2),p\mid m_1m_2$。由于 p 是一个素数，$(m_1,m_2)=1$，所以必有 $p\mid m_1$ 或者 $p\mid m_2$。不妨设 $p\mid m_1$，于是由 $p\mid(m_2x_1+m_1x_2)$ 和 $p\mid m_1$ 又得出 $p\mid m_2x_1$，由于 $(m_1,m_2)=1$，所以 p 不可能整除 m_2（否则 m_1,m_2 将有大于 1 的公因数 p），那么因此只能是 $p\mid x_1$，再由我们前面的假设 $p\mid m_1$ 就得出 x_1 与 m_1 有大于 1 的公因数 p。而这又与定理中 x_1 遍历 $0,1,2,\cdots,m_1-1$ 中所有与 m_1 互素的数的条件相矛盾。同理可证也不可能成立 $p\mid m_2$。这就证明了 r 与 m_1m_2 必然是互素的。

(2) 现在设 r 是 $0,1,2,\cdots,m_1m_2-1$ 中某一个与 m_1m_2 互素的数。那么由定理 3.7.3 所证明的结论可知，必存在两个整数 $x_1\in\{0,1,2,\cdots,m_1-1\}$，$x_2\in$

$\{0,1,2,\cdots,m_2-1\}$,使得

$$m_2x_1+m_1x_2\equiv r(\bmod m_1m_2)$$

我们现在证明 x_1 必定与 m_1 互素,x_2 必定与 m_2 互素。假设不然,不妨设 $(x_1,m_1)=d>1$,那么

$$(r,m_1)=(m_2x_1+m_1x_2-qm_1m_2,m_1)=(m_2x_1,m_1)=(x_1,m_1)=d>1$$

(这里最后一步用到了定理 3.3.10)。由于$(m_1,m_2)=1$,因此又有

$$(r,m_1m_2)=(r,m_1)=d>1$$

(这里又一次用到了定理 3.3.10)。而这与 r 是 $0,1,2,\cdots,m_1m_2-1$ 中某一个 m_1m_2 与互素的数的假设相矛盾,同理可证 x_2 必定与 m_2 互素。这就证明了 $0,1,2,\cdots,m_1m_2-1$ 中所有与 m_1m_2 互素的数都与一个形如 $m_2x_1+m_1x_2$ 的数同余。其中 x_1 与 m_1 互素,x_2 与 m_2 互素。

综合以上两方面的论述,就证明了当 x_1 遍历 $0,1,2,\cdots,m_1-1$ 中所有与 m_1 互素的数,x_2 遍历 $0,1,2,\cdots,m_2-1$ 中所有与 m_2 互素的数时,$m_2x_1+m_1x_2$ 被 m_1m_2 去除所得的余数就遍历了 $0,1,2,\cdots,m_1m_2-1$ 中所有与 m_1m_2 互素的数。

前面我们已经根据 $\varphi(m)$ 的定义通过验证得出

$$\varphi(1)=1,\varphi(2)=1,\varphi(3)=2,\varphi(4)=2,\varphi(5)=4,\varphi(6)=2$$

再验证一下,又可以得出

$$\varphi(7)=6,\varphi(8)=4,\varphi(9)=6,\varphi(10)=4,\varphi(11)=10,\varphi(12)=4$$

我们再试几个不同的底数 a,使得$(a,m)=1$,看看什么时候能有 $a^n\equiv 1(\bmod m)$,通过直接计算,不难算出一批例子如下

$2^2\equiv1(\bmod 3),2^4\equiv1(\bmod 5),2^6\equiv1(\bmod 7),2^6\equiv1(\bmod 9),2^{10}\equiv1(\bmod 11)$

$3^1\equiv1(\bmod 2),3^2\equiv1(\bmod 4),3^4\equiv1(\bmod 5),3^6\equiv1(\bmod 7),3^4\equiv1(\bmod 8)$

$5^2\equiv1(\bmod 6),5^6\equiv1(\bmod 7),5^4\equiv1(\bmod 8),5^6\equiv1(\bmod 9),5^4\equiv1(\bmod 12)$

通过对照这批例子和上面的欧拉函数的值不难发现,对于每一个底数,使 $a^n\equiv 1(\bmod m)$ 成立的指数恰好是模的欧拉函数的值,因此我们有理由猜想应成立公式

$$a^{\varphi(m)}\equiv1(\bmod m)$$

当然前提是$(a,m)=1$(因为如果 a 和 m 有公因数 $d>1$,因此有 $a=bd,m=cd$,那么对任一个 $k>1$,由 $m\mid(a^k-1)$,将得出 $a^k-1=qm,1=a^k-qm=(bd)^k-qcd,d\mid1$,而这是不可能的。这就是说如果 a 和 m 有公因数 $d>1$,那么对任一个 $k>1$,都不可能成立同余式 $a^k\equiv1(\bmod m)$)。

当然目前这还只是一个猜想,下面我们就来证明这一猜想。其实证明这一猜想的线索已包含在定理 3.7.1 中了。在那个定理中说"$r'_1,r'_2,\cdots,r'_{\varphi(m)}$ 只不过是 $r_1,r_2,\cdots,r_{\varphi(m)}$ 的一个排列",这是什么意思呢?这就是说,如果单个来看 r_i 和 r'_i,它们就是不一样的,但是如果把这两类数的集合作为一个整体看,它们

就是完全相同的，而一个以这些数作为变量的函数，如果不能分辨它们的区别，那这个函数在这两个集合上的值就是完全相同的。什么样的函数是不能分辨这些变量的呢？只要变量在这个函数中的地位是对称的，这个函数就无法分辨这些变量。这样的函数很多，其中最简单的例子是 $x_1 + x_2 + \cdots + x_{\varphi(m)}$ 和 $x_1 \cdot x_2 \cdots x_{\varphi(m)}$。我们一眼就看出如果把 $ar_1, ar_2, \cdots, ar_{\varphi(m)}$ 代入到这个函数中，就会出现 $a^{\varphi(m)}$ 这一项，这已经很像我们的猜想了，下一步就是认认真真地把这些想法严格地去实现出来。

定理 3.7.5(欧拉定理)　设 $(a,m) = 1, m \geqslant 2$，那么 $a^{\varphi(m)} \equiv 1 \pmod m$。

证明　设 $\{r_1, r_2, \cdots, r_{\varphi(m)}\}$ 是小于 m 且与 m 互素的正整数的集合，$\{r'_1, r'_2, \cdots, r'_{\varphi(m)}\}$ 是 $ar_1, ar_2, \cdots, ar_{\varphi(m)}$ 被 m 除所得的余数的集合，那么由定理 3.7.1 知 $r'_1, r'_2, \cdots, r'_{\varphi(m)}$ 只不过是 $r_1, r_2, \cdots, r_{\varphi(m)}$ 的一个重新排列。因此

$$a^{\varphi(m)}(r_1 \cdot r_2 \cdot \cdots \cdot r_{\varphi(m)}) \equiv ar_1 \cdot ar_2 \cdot \cdots \cdot ar_{\varphi(m)} \equiv$$
$$r'_1 \cdot r'_2 \cdot \cdots \cdot r'_{\varphi(m)} \equiv r_1 \cdot r_2 \cdot \cdots \cdot r_{\varphi(m)} \pmod m$$

由 $r_1, r_2, \cdots, r_{\varphi(m)}$ 的定义可知 $(r_i, m) = 1, i = 1, 2, \cdots, \varphi(m)$，因此由定理 3.3.10 可知 $(r_1 \cdot r_2 \cdot \cdots \cdot r_{\varphi(m)}, m) = 1$，因此由 3.6.4 中的性质(8)(即同余式的消去法则)即得

$$a^{\varphi(m)} \equiv 1 \pmod m$$

这就证明了定理。

欧拉定理只肯定了使得 $a^k \equiv 1 \pmod m$ 成立的指数的存在性，却并没有指出如何去计算这一指数，下面我们就来研究欧拉函数的计算问题。为此，首先证明欧拉函数的一个重要性质：

定理 3.7.6　如果 $(m,n) = 1$，那么 $\varphi(mn) = \varphi(m)\varphi(n)$。

证明　由定理 3.7.4 知当 x 遍历 $0, 1, 2, \cdots, m-1$ 中所有与 m 互素的数，y 遍历 $0, 1, 2, \cdots, n-1$ 中所有与 n 互素的数时，$nx + my$ 被 mn 去除所得的余数就遍历 $0, 1, 2, \cdots, mn-1$ 中所有与 mn 互素的数。

现在我们用两种方法来计算 $nx + my$ 所遍历的数的数目。一方面，$nx + my$ 所遍历的数由 nx 所遍历的数和 my 所遍历的数搭配而成，其中 nx 通过 $\varphi(m)$ 个数，my 通过 $\varphi(n)$ 个数，因此 $nx + my$ 共可搭配成 $\varphi(m)\varphi(n)$ 个数；另一方面，由定理 3.7.4 知 $nx + my$ 通过 $\varphi(mn)$ 个数。表示 $nx + my$ 所通过的数的数目的这两种式子当然应该是相等的，所以我们就得到 $\varphi(mn) = \varphi(m)\varphi(n)$。

在上面这个定理中，条件 $(m,n) = 1$ 是不可少的，例如 $\varphi(8) = 4, \varphi(2) = 1$，显然 $\varphi(8) \neq (\varphi(2))^3$。所以对 $\varphi(p^a)$，还要单独研究它的计算公式。对此，我们有

定理 3.7.7　对一切正整数成立 $\varphi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$。

证明　小于或等于 p^n 且与 p^n 不互素的正整数(也就是与 p^n 有大于 1 的共

因数的数）只有 p 的倍数 $1\cdot p, 2\cdot p, 3\cdot p, \cdots, (p^{n-1})\cdot p$，这些倍数一共有 p^{n-1} 个，剩下的数就都是 p^n 与互素的正整数了。而小于或等于 p^n 的正整数总共有 p^n 个，故我们有

$$\varphi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$$

综合定理 3.7.6 和 3.7.7 我们就可以推导出 $\varphi(m)$ 的计算公式了。

定理 3.7.8 若 n 的素因子分解式为 $n = p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}$，那么

$$\varphi(n) = p^{a_1-1}(p_1-1)p_2^{a_2-1}(p_2-1)\cdots p_k^{a_k-1}(p_k-1) =$$

$$n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)$$

证明 由于 $p_1^{a_1}, p_2^{a_2}, \cdots, p_k^{a_k}$ 是两两互素的，故用定理 3.7.6 可得

$$\varphi(n) = \varphi(p_1^{a_1})\varphi(p_2^{a_2})\cdots\varphi(p_k^{a_k})$$

对右端的各个因子再应用定理 3.7.7 和进行简单的恒等式变形即可证明定理 3.7.8。

知道如何计算欧拉函数的值之后，欧拉定理实际上还可以加强。这就是下面的加强型的欧拉定理：

定理 3.7.9 设 $(a,m)=1$，$m = p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}$ 是 m 的素因子分解式

$$l(m) = [\varphi(p_1^{a_1})\varphi(p_2^{a_2})\cdots\varphi(p_k^{a_k})]$$

是 $\varphi(p_1^{a_1})\varphi(p_2^{a_2}),\cdots,\varphi(p_k^{a_k})$ 的最小公倍数。则

$$a^{l(m)} \equiv 1 (\bmod\ m)$$

证明 由于 $(a,m)=1$，故 $(a,p_i^{a_i})=1, i=1,2,\cdots,k$。因此由欧拉定理得

$$a^{\varphi(p_i^{a_i})} \equiv 1(\bmod\ p_i^{a_i}), i = 1,2,\cdots,k$$

将上面的同余式两边分别乘方 $\dfrac{l(m)}{\varphi(p_i^{a_i})}$ 次，即得 $a^{l(m)} \equiv 1(\bmod\ p_i^{a_i})$。再由于 $p_1^{a_1}$，$p_2^{a_2},\cdots,p_k^{a_k}$ 是两两互素的，因此由同余式的性质定理 3.6.4(a) 即得

$$a^{l(m)} \equiv 1(\bmod\ p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}) \equiv 1(\bmod\ m)$$

这就证明了定理。

由于 $\varphi(m)$ 显然是 $l(m)$ 的倍数，所以从定理 3.7.9 可以推出欧拉定理，因此定理 3.7.9 要比欧拉定理更强一些。

由上面几个定理立即得出下面的欧拉定理的特例：

定理 3.7.10(费马小定理) 设 p 是一个素数，a 是一个整数，$(a,p)=1$，则

$$a^{p-1} \equiv 1(\bmod\ p)$$

证明 容易算出来 $\varphi(p) = p-1$，这就证明了定理。

下面我们再来证明一个欧拉函数的性质：

定理3.7.11 设 n 是一个正整数,则 $\sum_{d|n}\varphi(d)=n$。这里的下标 $d\mid n$ 表示 d 通过 n 的所有正的因子。

证明 首先想到的当然是应用欧拉函数的计算公式,但是马上你会发现这并不轻松(当然也可以用这一路线去证明这一定理,但总之会出现让人头疼的复杂公式)。幸亏大数学家高斯早就想出了一个巧妙的证明方法(看完这个证明以后,你不得不佩服高斯确实是一个眼光敏锐、头脑机灵的数学天才)。

高斯的方法其实我们已经见过,就是把数分类。关键是怎么分类可不好想,这里的关键是要有敏锐的眼光,能看出来分类的原则。

对整数 $1,2,3,\cdots,n$,我们定义集合 C_d 的含义为 $C_d=\{k\mid(k,n)=d\}$,也就是按 $1,2,3,\cdots,n$ 中每个数 k 和 n 的最大公约数是多少来把 $1,2,3,\cdots,n$ 中的数加以分类。例如设 $n=12$,那么由于12的约数共有1,2,3,4,6,12这6个数,所以 $1,2,3,\cdots,12$ 这12个数共可分成6类数如下

$$C_1=\{1,5,7,11\},C_2=\{2,10\},C_3=\{3,9\},C_4=\{4,8\},C_6=\{6\},C_{12}=\{12\}$$

现在我们可以看出三个问题,首先就是说是按 $1,2,3,\cdots,n$ 中每个数 k 和 n 的最大公约数是多少来把 $1,2,3,\cdots,n$ 中的数加以分类,其实也是按照 n 的约数来把 $1,2,3,\cdots,n$ 中的数加以分类。看出这一点后,你对高斯为什么要这么分类有点琢磨出味来了吧,你要证的式子中有 n 的约数,你现在搞的这种分类里也出现了 n 的约数,这就把两边挂上钩了。其次是这样定义出来的类中没有空集,因为至少 n 的约数 d 本身是属于集合 C_d 的。第三由于最大公约数是唯一的,因此不同的类是两两不相交的。也就是说小于或等于 n 的任一数必属于且仅属于某一个类。

最后,我们要关注的问题是,类 C_d 中究竟有多少个元素?设 C_d 的势为 x(回忆一个有限集合的势就是这个集合中元素的个数)。由于

$$k\in C_d\Leftrightarrow(k,n)=d\Leftrightarrow\left(\frac{k}{d},\frac{n}{d}\right)=1$$

因此如果 C_d 中有一个元素 k,那么就存在一个和 $\frac{n}{d}$ 互素的数,这就是说至少有 x 个数和 $\frac{n}{d}$ 互素,即 $x\leqslant\varphi\left(\frac{n}{d}\right)$;反过来,如果有一个数 k 和 $\frac{n}{d}$ 互素,那么由上面的式子可知,就有一个数 $dk\in C_d$,也就是说,C_d 中至少有 $\varphi\left(\frac{n}{d}\right)$ 个元素,即 $x\geqslant\varphi\left(\frac{n}{d}\right)$。综合以上两方面的论述就有 $|C_d|=\varphi\left(\frac{n}{d}\right)$(这里 C_d 表示集合 C_d 的势)。因此最后由集合的分解式 $\{1,2,3,\cdots,n\}=\bigcup_{d|n}C_d$ 与有限集合势的计算公式(注意集合 C_d 是两两不相交的)。就得到 $|\{1,2,3,\cdots,n\}|=\sum_{d|n}|C_d|$,再把

$|C_d| = \varphi\left(\frac{n}{d}\right)$代入前面的式子就得出

$$n = \sum_{d|n}\varphi\left(\frac{n}{d}\right)$$

习题 3.7

1. 设 p 是一个素数,证明:$\varphi(1) + \varphi(p) + \cdots + \varphi(p^a) = p^a$。

2. 证明:如果 n 是奇数,则 $\varphi(4n) = 2\varphi(n)$。

3. 证明:

(1) $\varphi(n^2) > (\varphi(n))^2$;

(2) 如果 m,n 有大于 1 的共因数,则 $\varphi(mn) > \varphi(m)\varphi(n)$。

4. 证明:如果$(m,n) = 2$,则 $\varphi(mn) = 2\varphi(m)\varphi(n)$。

5. 证明:$\varphi(n) = \frac{n}{2}$ 的充分必要条件是 $n = 2^k$。

6. 证明:$\varphi(n) = \frac{n}{3}$ 的充分必要条件是 $n = 2^k \cdot 3^l$。

7. (1) 证明:如果 $6 | n$,则 $\varphi(n) \leqslant \frac{n}{3}$;

(2) 如果连续两个奇数 $n, n+2$ 都是素数,则称 $n, n+2$ 是一对孪生素数,证明:$n, n+2$ 是一对大于 4 的孪生素数的必要条件是 n 必须满足不等式

$$\varphi(n+1) \leqslant \frac{n+1}{3}$$

8. 证明:不存在正整数 n 使得 $\varphi(n) = 14$。

9. 设 $n > 1$,$f(n)$ 表示所有不超过 n 且与 n 互素的正整数之和。证明:如果 $f(m) = f(n)$,则 $m = n$。

10. 设 $a > 1$,p 是大于 2 的素数,证明:

(1) 如果 q 是 $a^p - 1$ 的素因数,则 q 是 $a - 1$ 的因数或者 $q \equiv 1 \pmod{2p}$;

(2) 如果 q 是 $a^p + 1$ 的素因数,则 q 是 $a + 1$ 的因数或者 $q \equiv 1 \pmod{2p}$;

(3) 设 p 是一个任意的素数,s 是一个任意的正整数。$a = 2^{p^{s-1}}$,q 是$\frac{a^p - 1}{a - 1}$的素因数,证明 $q = 2k \cdot p^s + 1$,其中 k 是某个正整数,从而证明存在无穷多个形如 $2kp + 1$ 的素数。

11. 设 p 是一个素数,证明:如果 q 是 $2^p - 1$ 的一个因数,则

(1) $q \equiv 1 \pmod{p}$;

(2) $q \equiv \pm 1 \pmod{8}$。

12. 证明:如果 q 是 $F_k = 2^{2^k+1}$ 的一个正因数,则

(1) $q \equiv 1 \pmod{2^{k+1}}$;

(2) 如果 $k \geqslant 2$,则 $q \equiv 1 \pmod{2^{k+2}}$。

13. 由以下数据

$$1+2=\frac{3}{2}\varphi(3),1+3=\frac{4}{2}\varphi(4),1+2+3+4=\frac{5}{2}\varphi(5)$$

$$1+5=\frac{6}{2}\varphi(6),1+2+3+4+5+6=\frac{7}{2}\varphi(7)$$

$$1+3+5+7=\frac{8}{2}\varphi(8)$$

猜想一个定理。并再用其他数据加强或者否定你的猜想,最后证明你的猜想。

14. 对下列情况:

(1) $n=12,13,14,15,16$;

(2) $n=p$,p 是一个奇素数;

(3) $n=2^k,k\geqslant 1$;

(4) $n=p^k,k\geqslant 1$,p 是一个奇素数。

计算式子 $\sum_{d\mid n}(-1)^{\frac{n}{d}}\varphi(d)$ 的值,并猜想一个定理,最后证明你的猜想。

15. 求 $(12\,371^{56}+34)^{28}$ 被 111 去除所得的余数。

16. $1\,093^2$ 是否能整除 $2^{1\,093}-2$?

17. 设 $(a,m)=1$,$x\equiv ca^{\varphi(m)-1} \pmod m$,则 $ax\equiv c \pmod m$。

3.8 整数的函数

在上一节中,我们引进了欧拉函数的概念,这是一个对每一个正整数都有定义的函数。像这样的函数就称为整数的函数。为了研究整数的性质,还有很多像这样的有趣的和有用的整数的函数,例如一个正整数的阶乘 $n!$,前 n 个自然数的最小公倍数 d_n 等等。我们先从最简单的函数开始介绍。

欧拉(Euler, Léonard, 1707—1783),瑞士数学家. 生于瑞士的巴塞尔,卒于彼得堡.

首先介绍一个实数的整数部分所定义的函数:

定义 3.8.1 设 x 表示一个任意的实数,则 $[x]$ 表示不大于 x 的最大整数。这一定义和以下几种说法都是等价的:

(1) $[x]$ 是 x 的整数部分;

(2) $[x]$ 是满足不等式 $x-1<[x]\leqslant x$ 的唯一整数;

(3) 在实数轴上写出实数 x,然后向左走,所碰见的的一个整数就是 $[x]$;

(4) $[x]$ 是满足不等式 $[x]\leqslant x<[x]+1$ 的唯一整数;

(5) $[x]$ 是 x 的地板,也可以记为 $\lfloor x\rfloor$。

例如，$[2]=2,\left[\frac{5}{2}\right]=2,[\pi]=3,\cdots$ 等等，通过这几个例子，你很容易掌握一个正数的整数部分是什么意思。下面我们举几个负数的整数部分的例子，读者一定要一开始就搞清楚，否则以后老要查书很是麻烦，我见过几个人，正数的整数部分理解得很清楚，可是一求负数的整数部分，他们就要翻书，老是记不住。注意看 $\left[-\frac{1}{2}\right]=-1,[-\pi]=-4$。因此 $[-1.2]$ 的整数部分是 -2，而不是 -1。所以如果你追求定义的直观性，你最好把 $[x]$ 称为 x 的地板，这样一想就清楚，决不会弄错。

与 x 的整数部分紧密相连的另一概念是 x 的分数部分。

定义 3.8.2 称 $x-[x]$ 为 x 的分数部分，记为 $\{x\}$。

由定义立刻可以得出这两个函数的一些最初级的性质如下：

引理 3.8.1 $[x]$ 和 $\{x\}$ 具有以下性质：

(1) $x=[x]+\{x\}$；

(2) $[-x]=\begin{cases}-[x]-1,\text{如果 } x \text{ 不是整数;}\\ -[x],\text{如果 } x \text{ 不是整数}\end{cases}$

(3) $[n+x]=n+[x]$，其中 n 是一个整数；

(4) $[x+y]\leqslant[x]+[y],\{x\}+\{y\}\geqslant\{x+y\}$。

(5) 设 a,b 是两个整数，$b>0$，则在 a 除以 b 的带余数除法公式

$$a=bq+r,0\leqslant r<b$$

中

$$q=\left[\frac{a}{b}\right]$$

(6) 设 a,b 是两个任意的正整数，则 b 的小于或者等于 a 的正的倍数的个数为

$$\left[\frac{a}{b}\right]$$

证明：我们只证明(5)和(6)。

(5) 的证明，按照带余数除法的证明(见定理 3.2.3)，整数 a 必定落在两个整数 qb 和 $(q+1)b$ 之间，使得 $qb\leqslant a<q+1$，于是我们称 q 是商，称 $r=a-qb$ 是余数。也就是说 q 是满足条件 $qb\leqslant a<q+1$ 的唯一整数。由此条件得 $q\leqslant\frac{a}{b}<q+1$，而按照地板函数的定义就知道

$$q=\left[\frac{a}{b}\right]$$

(6) 的证明，当 $a<b$ 时，此性质显然成立。以下设 $a>b$。

再设所有 b 的小于或者等于 a 的正的倍数为 $b,2b,3b,\cdots,mb$。则由于这些倍数都小于或等于 a，因此我们有 $0<bm\leqslant a$，故

$$0 < m \leqslant \frac{a}{b}$$

另一方面,按照最大的定义,接在 mb 后面的下一个 b 的倍数要大于 a,即

$$(m+1)b > a$$

或者

$$\frac{a}{b} < m + 1$$

联合上面两个不等式就得到

$$m \leqslant \frac{a}{b} < m + 1$$

再根据$\left[\frac{a}{b}\right]$的定义即可知所有满足条件的 b 的倍数 bm 的个数 m 就等于$\left[\frac{a}{b}\right]$。这就证明了引理。

受到上面$[x]$就是 x 的地板函数的定义的启发,我们也可以定义 x 的天花板。

定义 3.8.3 设 x 是一个任意实数,则称满足条件 $n < x \leqslant n+1$ 的唯一整数 n 为 x 的天花板,记为 $\lceil x \rceil$。

另一个启发是带余数除法的定义其实可以推广,按照直观的感觉,余数就是剩下的东西的个数,当然不会是负数。但是如果纯从公式 $a = bq + r$ 来看,似乎就没有必要一定需要这个限制因为余数这个概念只依赖于商的选取方法,你既然可以选取 x 的地板做为商,为什么就不能选取 x 的天花板做为商呢,从纯数学的角度来看,这两个数的地位是完全平等的。事实上,我们还可以有的时候选取 x 的地板作为商,有的时候选取 x 的天花板作为商。这就引出另一种带余数除法。

定理 3.8.1(第二带余数除法) 设 a, b 是两个整数, $b \neq 0$,则存在两个整数 q 及 r 使得

$$a = bq + r, |r| \leqslant \frac{|b|}{2}$$

证明 实数$\frac{a}{b}$必位于两个相邻的整数之间,即存在一个整数 n 使得

$$n \leqslant \frac{a}{b} \leqslant n + 1$$

现在选取 q 是距离$\frac{a}{b}$最近的整数,即当 $0 \leqslant \frac{a}{b} - n \leqslant \frac{1}{2}$ 时,选取 $q = n$,当 $0 \leqslant n + 1 - \frac{a}{b} \leqslant \frac{1}{2}$ 时,选取 $q = n + 1$。再令 $r = a - bq$,于是显然就有 $a = bq + r$。再按照 q 的选取方法知 $\left|\frac{r}{b}\right| = \left|\frac{a}{b} - q\right| \leqslant \frac{1}{2}$,故必有 $|r| \leqslant \frac{|b|}{2}$。这就证明了定理。

显然，在第二带余数除法中，余数的唯一性不再具有，例如，如果 $a = 7$，$b = 2$，那么你既可以取 $q = 3$，也可以取 $q = 4$。在取 $q = 3$ 的情况下，余数 $r = a - bq = 1$；在取 $q = 4$ 的情况下余数 $r = a - bq = -1$。

有的人可能要问，既然有了通常的带余数除法，为什么还要证明这个结论更弱的第二带余数除法呢？回答是，在目前的阶段，第二带余数除法的结论确实比通常的带余数除法弱，但是这两个定理的区别在于，第二带余数除法的结论不依赖于余数的大小这一概念，这就使得它将来有可能推广到更一般的情况下，即对任何成立第二带余数除法的"整数"，我们都可以实行类似于普通整数的辗转相除法。

关于带余数除法还要说明的一点是，尽管当初得出带余数除法定理时，我们是对整数定义的，但是如果你仔细琢磨这个定理的证明就会发现，其实我们可以对任何实数 a 和任何正数 b 证明一般的带余数除法定理如下。

一般的带余数除法定理　设 a 是任意实数，b 是任意正数，那么必存在唯一的整数 q 和实数 r 使得 $a = bq + r, 0 \leqslant r < b$。

从这个一般的带余数除法出发，你一样可以定义一个称为辗转相除法的程序或算法，但是这回，由于 r 不一定是整数，你定义的这个算法就不一定在有限步内结束了。

下面我们利用 x 的地板这一概念来得出一些表示式，为此需先证明一个简单的引理。

引理 3.8.2　对任何正整数 n，$\left[\frac{[x]}{n}\right] = \left[\frac{x}{n}\right]$ 成立。

证明　由带余数除法知对整数 $[x]$ 和 n 成立关系式

$$[x] = qn + r, 0 \leqslant r < n$$

或者

$$\frac{[x]}{n} = q + \frac{r}{n}, 0 \leqslant \frac{r}{n} < 1$$

由此得出

$$\left[\frac{[x]}{n}\right] = q$$

另一方面又有

$$\frac{x}{n} = \frac{[x]}{n} + \frac{\{x\}}{n} = q + \frac{\{x\} + r}{n}$$

利用 r 是一个整数的下述特性，即可由 $0 \leqslant r < n$ 得出 $0 \leqslant r \leqslant n - 1$，以及 $\{x\}$ 的下述特性 $0 \leqslant \{x\} < 1$ 就可得出 $0 \leqslant \{x\} + r < n$，因此

$$0 \leqslant \frac{\{x\} + r}{n} < 1$$

从地板函数的定义最后就得出

$$\left[\frac{x}{n}\right] = q = \left[\frac{[x]}{n}\right]$$

这就证明了引理。

利用这一引理和引理 3.8.1 的性质(6) 就可以证明下面的关于 $n!$表达式。

定理 3.8.2 在 $n!$的素因数分解式中，素数 p 的指数 $\alpha(p,n)$ 的值为

$$\alpha(p,n)=\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\cdots=\sum_{k=1}^{\infty}\left[\frac{n}{p^k}\right]$$

证明 在 $A=1\cdot 2\cdot\cdots\cdot n=n!$中共有$\left[\frac{n}{p}\right]$个 p 的倍数，即 $p,2p,3p,\cdots,\left[\frac{n}{p}\right]p$。除此之外，$n!$中就没有别的能被 p 整除的因数了。把这些因数相乘就得到

$$p\cdot 2p\cdot 3p\cdot\cdots\cdot\left[\frac{n}{p}\right]p=\left[\frac{n}{p}\right]!\,p^{\left[\frac{n}{p}\right]}=A_1p^{\left[\frac{n}{p}\right]}$$

因此，我们已从 $A=n!$中分出了一部分 p 的乘幂$p^{\left[\frac{n}{p}\right]}$，但是在 A_1 中还有另一部分 p 的乘幂。因此我们还需计算 A_1 中有多少 p 的乘幂。由于 A_1 具有和 A 完全相同的形式，因此重复刚才的论证就知道 A_1 中含有 p 的乘幂的部分为

$$\left[\frac{\left[\frac{n}{p}\right]}{p}\right]=\left[\frac{\left[\frac{n}{p}\right]}{p}\right]!\,p^{\left[\frac{\left[\frac{n}{p}\right]}{p}\right]}$$

由引理 3.8.2 可知

$$\left[\frac{\left[\frac{n}{p}\right]}{p}\right]=\left[\frac{n}{p^2}\right]$$

因此 A_1 中含有 p 的乘幂的部分就是

$$\left[\frac{n}{p^2}\right]!\,p^{\left[\frac{n}{p^2}\right]}=A_2p^{\left[\frac{n}{p^2}\right]}$$

这样我们又从 $A=n!$中分出一部分 p 的乘幂为$p^{\left[\frac{n}{p^2}\right]}$，其他的 p 的乘幂只可能包含在 A_2 中，而 A_2 又具有和 A_1 完全相同的形式，因此重复进行上述讨论，就可分出 p 的所有乘幂为$p^{\left[\frac{n}{p}\right]},p^{\left[\frac{n}{p^2}\right]},p^{\left[\frac{n}{p^3}\right]},\cdots$因而在 $n!$的素因子分解式中，p 的指数即为上述所有这些 p 的乘幂的指数之和，也就是说

$$\alpha(p,n)=\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\cdots=\sum_{k=1}^{\infty}\left[\frac{n}{p^k}\right]$$

上面的表示式虽然是一个无穷的和，实际上只包含有限项，因为显然当 k 充分大时，求和号后面的表达式就变成零了。

例 3.8.1 证明：$2^{47}\mid 50!$。

证明 只要算出 50!中包含有多少 2 的乘幂即可，由上面的定理知

$$\alpha(2,50)=\left[\frac{50}{2}\right]+\left[\frac{50}{4}\right]+\left[\frac{50}{8}\right]+\left[\frac{50}{16}\right]+\left[\frac{50}{32}\right]=$$

$$25 + 12 + 6 + 3 + 1 = 47$$

故 $2^{47} \mid 50!$。

例 3.8.2 求 21!的素因子分解式。

解 不超过 21 的素数有 2,3,5,7,11,13,17,19。因此由上面的定理知

$$\alpha(2,21) = \left[\frac{21}{2}\right] + \left[\frac{21}{4}\right] + \left[\frac{21}{8}\right] + \left[\frac{21}{16}\right] =$$

$$10 + 5 + 2 + 1 = 18$$

$$\alpha(3,21) = \left[\frac{21}{3}\right] + \left[\frac{21}{9}\right] = 7 + 2 = 9$$

$$\alpha(5,21) = \left[\frac{21}{5}\right] = 4, \alpha(7,21) = \left[\frac{21}{7}\right] = 3$$

$$\alpha(11,21) = \left[\frac{21}{11}\right] = 1, \alpha(13,21) = \left[\frac{21}{13}\right] = 1$$

$$\alpha(17,21) = \left[\frac{21}{17}\right] = 1, \alpha(19,21) = \left[\frac{21}{19}\right] = 1$$

所以

$$21! = 2^{18}3^9 \cdot 5^4 \cdot 7^3 \cdot 11 \cdot 13 \cdot 17 \cdot 19$$

例 3.8.3 证明 $[x] + [2x] = 5$ 没有实数解。

证明 设 $f(x) = [x] + [2x]$,则显然有

(1) $f(x)$ 是不减的函数;

(2) $f(x + n) = f(x) + f(n) = f(x) + 3n$,其中 n 是一个整数。

又 $f(1) = 3, f(2) = 6$,故 $f(1) < 5 < f(2)$,因而 $1 < x < 2$。令 $y = x - 1$,则 $0 < y < 1$。因此 $[y] = 0, 0 < [2y] < 1$,故

$$f(y) = [y] + [2y] < 1$$

但是另一方面又有

$$f(y) = f(x) - f(1) = 5 - 3 = 2$$

这是一个矛盾,所得的矛盾就证明了 $f(x) = 5$ 没有实数解。

在坐标系中横坐标和纵坐标都是整数的点称为整点或格点,计算某一区域内包含有多少个整点是一个既有数学兴趣又有实际意义的问题,比如,这种计算格点的公式在林业中可用来估计某一区域内树木的棵数,预计森林成长的速度等等。下面我们就用地板函数给出一个这种公式。

定理 3.8.3 如图 3.8.1。

(1) 设 $f(x)$ 在区间 $Q \leqslant x \leqslant R$ 中是连续而且非负的,则和式

$$\sum_{Q<x<R} [f(x)]$$

表示在范围 $Q < x < R, 0 < y \leqslant f(x)$ 里的格点的个数。(求和号中 $Q < x < R$ 的表示 x 通过区间 $Q < x < R$ 中所有的整数)

(2) 设 $g(y)$ 在区间 $N \leqslant y \leqslant M$ 中是连续而且非负的,则和式

$\sum\limits_{N<y<M}[g(y)]$ 表示在范围 $N<y<M, 0<x\leqslant g(y)$ 里的格点的个数。(求和号中 $N<y<M$ 的表示 y 通过区间 $N<y<M$ 中所有的整数)

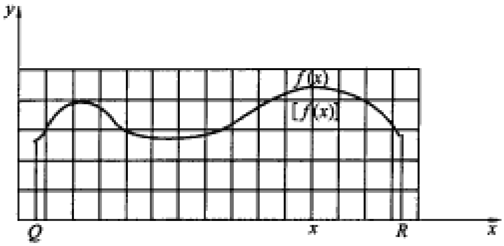


图 3.8.1

证明　(1) 设 T 表示范围 $Q\leqslant x\leqslant R, 0<y\leqslant f(x)$ 里的格点的个数。那么此范围内的格点由适合条件 $Q\leqslant x\leqslant R$, x 是整数的那些 x 做横坐标的直线上所有在 $f(x)$ 下面的格点所组成。在这条直线上,从 $y=1$ 数起共有 $[f(x)]$ 个格点,故

$$T=\sum_{Q<x<R}[f(x)]$$

(2) 可类似证明,不过刚才是竖着数,现在是横着数。

注意 T 不包括所有横轴上和两边上的格点。

现在我们就用这个定理来证明一个有趣的等式。

定理 3.8.4　设 p 和 q 是不同的奇素数,则

$$\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{kq}{p}\right]+\sum_{k=1}^{\frac{q-1}{2}}\left[\frac{kp}{q}\right]=\frac{p-1}{2}\cdot\frac{q-1}{2}$$

证明　如图 3.8.2。

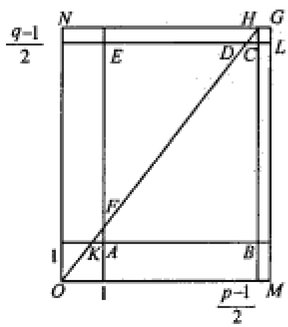


图 3.8.2

设 $M=\frac{p-1}{2}+\epsilon, N=\frac{q-1}{2}+\epsilon$，其中 ϵ 是一个充分小的数。

设点 A 的坐标是 $(1,1)$，点 B 的坐标是 $\left(\frac{p-1}{2},1\right)$，点 C 的坐标是 $\left(\frac{p-1}{2},\frac{q-1}{2}\right)$，点 E 的坐标是 $\left(1,\frac{q-1}{2}\right)$。又设直线 $y=\frac{q}{p}x$ 与直线 $y=1$ 交于点 K，与直线 $x=1$ 交于点 F，与直线 $y=\frac{q-1}{2}$ 交于点 D，与直线 $y=N$ 交于点 H，直线 $x=M$ 与直线 $y=N$ 交于点 G，直线 $y=\frac{q-1}{2}$ 与直线 $x=M$ 交于点 L。那么

$$T=\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{kq}{p}\right]+\sum_{k=1}^{\frac{q-1}{2}}\left[\frac{kp}{q}\right]=\sum_{0<x<M}\left[\frac{q}{p}x\right]+\sum_{0<y<N}\left[\frac{p}{q}y\right]=S(p,q)+S(q,p)$$

按照定理 3.8.3，$S(p,q)$ 表示区域 $0<x<M, 0<\frac{q}{p}x<N$ 内的格点数，也就是多边形 $OMGN$ 内部的格点。注意由于 p,q 都是素数，所以在矩形 $OMGN$ 内部，直线 $y=\frac{q}{p}x$ 上除了原点之外是没有其他格点的。另外由于 ϵ 是充分小的数，因此在多边形 $DLGH$ 和 KAF 内部及边界上，除了点 C 之外没有其他格点。这就是说 $S(p,q)$ 就表示多边形 $ABCDEF$ 内部及边界上的所有格点的数目。而且 FD 边上没有格点。

注意 $y=\frac{q}{b}x$ 方程和方程 $x=\frac{p}{q}y$ 表示同一条直线，因此用完全与上面类似的论述就可说明 $S(q,p)$ 表示 $\triangle DEF$ 内部及边界上的格点的数目。

再注意多边形 $ABCDEF$ 和 $\triangle DEF$ 的公共部分线段 FD 上没有任何格点。因此 $S(p,q)+S(q,p)$ 就表示这两个区域的并集，即矩形 $ABCE$ 内部及边界上的全部格点数。而一个矩形的内部及边界上共有多少个格点是很容易计算的。实际上，AB 边上共有 $\frac{p-1}{2}$ 个格点，AE 边上共有 $\frac{q-1}{2}$ 个格点，因此矩形 $ABCE$ 内部及边界上的全部格点数就是这两个数相乘的乘积。故最后我们就得到

$$T=S(p,q)+S(q,p)=\frac{p-1}{2}\cdot\frac{q-1}{2}$$

这个定理的有趣之处就在于直接求 T 是不容易的，而在定理 3.8.3 赋予了 $S(p,q)$ 和 $S(q,p)$ 以几何意义后，利用图形就巧妙地求出了本来没有办法求出来的和。目前它也不过就是一个巧妙的拼图游戏而已，它背后的更深刻的意义，要在二次剩余中的互反律中才能表现出来。

尽管定理 3.8.3 可以赋予某种和以几何意义，但是矩形毕竟是一种太特殊的图形了，要能更广泛地应用定理 3.8.3，我们还必须有更有力的工具配合它才行。这就是下面要讲的欧拉求和公式。

定理 3.8.5(欧拉求和公式)

(1)
$$\sum_{a<n\leqslant b} f(n)=\int_a^b f(x)\mathrm{d}x+\int_a^b\left(x-[x]-\frac{1}{2}\right)f'(x)\mathrm{d}x+\left(a-[a]-\frac{1}{2}\right)f(a)-\left(b-[b]-\frac{1}{2}\right)f(b)$$

(2)
$$\sum_{k=1}^{n} f(k)=\int_1^n f(x)\mathrm{d}x+\frac{1}{2}(f(n)+f(1))+\int_1^n B_1(\{x\})f'(x)\mathrm{d}x$$

证明 (1) 分下列两种情况证明。

(i) $[a]+1>[b]$;

这时由于 $a<b$,故 $[a]\leqslant[b]<[a]+1$,因此 $[a]=[b]$。这说明在区间 $a<n\leqslant b$ 中根本没有整数,所以 $T=\sum\limits_{a<n\leqslant b}f(n)=0$,且在区间 $[a,b]$ 上,$[x]=[a]$。故由分部积分公式得出

$$\begin{aligned}\int_a^b\left(x-[x]-\frac{1}{2}\right)f'(x)\mathrm{d}x&=\left(x-[a]-\frac{1}{2}\right)f(x)\Big|_a^b-\int_a^b f(x)\mathrm{d}x=\\&\left(b-[a]-\frac{1}{2}\right)f(b)-\\&\left(a-[a]-\frac{1}{2}\right)f(a)-\int_a^b f(x)\mathrm{d}x=\\&\left(b-[b]-\frac{1}{2}\right)f(b)-\\&\left(a-[a]-\frac{1}{2}\right)f(a)-\int_a^b f(x)\mathrm{d}x\end{aligned}$$

故

$$\int_a^b f(x)\mathrm{d}x+\int_a^b\left(x-[x]-\frac{1}{2}\right)f'(x)\mathrm{d}x+\left(a-[a]-\frac{1}{2}\right)f(a)-\left(b-[b]-\frac{1}{2}\right)f(b)=0=T$$

这就证明了定理的结论对情况(i)是成立的。

(ii) $[a]+1<[b]$。这时

$$\begin{aligned}\int_a^b[x]f'(x)\mathrm{d}x&=\left(\int_a^{[a]+1}+\int_{[a]+1}^{[a]+2}+\cdots+\int_{[b]-1}^{[b]}+\int_{[b]}^{b}\right)[x]f'(x)\mathrm{d}x=\\&\int_a^{[a]+1}[a]f'(x)\mathrm{d}x+\int_{[b]}^{b}[b]f'(x)\mathrm{d}x+\\&\left(\int_{[a]+1}^{[a]+2}([a]+1)+\int_{[a]+2}^{[a]+3}([a]+2)+\cdots+\right.\\&\left.\int_{[b]-1}^{[b]}([b]-2)\right)f'(x)\mathrm{d}x=\\&\sum_{n=[a]+1}^{[b]-1}\int_n^{n+1}nf'(x)\mathrm{d}x+\int_a^{[a]+1}[a]f'\mathrm{d}x+\int_{[b]}^{b}[b]f'(x)\mathrm{d}x=\end{aligned}$$

$$\sum_{n=[a]+1}^{[b]-1} n(f(n+1)-f(n)) + (f([a]+1)-f(a))[a] +$$
$$(f(b)-f([b]))[b] =$$
$$-\sum_{n=[a]+1}^{[b]} f(n) + [b]f(b) - [a]f(a) =$$
$$-\sum_{a<n\leqslant b} f(n) + [b]f(b) - [a]f(a)$$

又由分部积分得

$$\int_a^b\left(x-\frac{1}{2}\right)f'(x)\mathrm{d}x = \left(x-\frac{1}{2}\right)f(x)\Big|_a^b - \int_a^b f(x)\mathrm{d}x =$$
$$\left(b-\frac{1}{2}\right)f(b) - \left(a-\frac{1}{2}\right)f(a) - \int_a^b f(x)\mathrm{d}x$$

因此把上面两式相加就得到

$$\int_a^b\left(x-[x]-\frac{1}{2}\right)f'(x)\mathrm{d}x = \int_a^b\left(x-\frac{1}{2}\right)f'(x)\mathrm{d}x - \int_a^b [x]f'(x)\mathrm{d}x =$$
$$\sum_{a<n\leqslant b} f(n) - [b]f(b) + [a]f(a) +$$
$$\left(b-\frac{1}{2}\right)f(b) - \left(a-\frac{1}{2}\right)f(a) - \int_a^b f(x)\mathrm{d}x$$

移项之后就得到我们所要证的式子。

因此综合(i),(ii) 两种情况,就证明了定理的结论。

如果令 $B_1(x) = x - \dfrac{1}{2}$,那么欧拉求和公式又可表示为

$$\sum_{a<n\leqslant b} f(n) = \int_a^b f(x)\mathrm{d}x - B_1(\{x\})f(x)\Big|_a^b + \int_a^b B_1(\{x\})f'(x)\mathrm{d}x$$

但是要注意,这种形式的欧拉求和公式的左边与我们通常的级数求和表示法有些不一致,它不包括第一项,为了得出与通常习惯上相一致的求和公式,我们令 $a = 1, b = n$,并且再加上第一项 $f(1)$ 就得到定理 3.8.5 中(2) 的公式。

$$\sum_{k=1}^{n} f(k) = f(1) + \sum_{1<k\leqslant n} f(k) =$$
$$f(1) + \int_1^n f(x)\mathrm{d}x + \frac{1}{2}(f(n)-f(1)) + \int_1^n \left(x-[x]-\frac{1}{2}\right)f'(x)\mathrm{d}x =$$
$$\int_1^n f(x)\mathrm{d}x + \frac{1}{2}(f(n)+f(1))\int_1^n B_1(\{x\})f'(x)\mathrm{d}x$$

再设 $\sigma(x) = \int_0^x B_1(\{x\})\mathrm{d}x$,并对$\int_a^b B_1(\{x\})f'(x)\mathrm{d}x$ 再做一次分部积分就可以得到带有二次导数的欧拉求和公式如下,又称为梭宁公式。

定理 3.8.6 设 $\sigma(x) = \int_0^x B_1(\{x\})\mathrm{d}x$,则

$$\sum_{Q<x\leqslant R} f(x) = \int_Q^R f(x)\mathrm{d}x - B_1(\{x\})f(x)\mid_Q^R + B_1(\{x\})f'(x)\mid_Q^R - \int_Q^R \sigma(x)f''(x)\mathrm{d}x$$

上面的这些公式在估计各种和数时是很有用的工具，例如在圆内整点问题中就可以得到应用。但是为了得到关于圆内整点问题的结果，除了上述公式外，还需要用到其他的辅助估计，例如对某种形式的小数部分的和的估计，所以我们就不在这具体讲这种应用的例子了，有兴趣的读者可以去看华罗庚写的《数论导引》或维诺格拉多夫写的《数论基础》这两本书。但是为了使读者对什么是圆内整点问题有一个大致的了解，我们还是对此问题稍微介绍一下。

所谓圆内整点问题就是要估计坐标系中以原点为圆心，半径是 r 的圆 $x^2+y^2=r^2$ 内部及边界上的整点的数目，也就是平面区域 $x^2+y^2\leqslant r^2$ 中的整点数目 $A(r)$。我们上面把圆的方程写成 $x^2+y^2=r^2$ 的形式是为了和通常表示圆的方程的习惯相统一，可以一眼就看出圆的圆心和半径。但是在研究圆内整点问题时，这样写反而不方便。因为这个整点的数目显然是依赖于方程右边的数的，所以在研究圆内整点问题时，习惯上用 $A(r)$ 表示平面区域 $x^2+y^2\leqslant r$ 中的整点数目，这点请读者注意。

如果我们把圆的大小固定，而把坐标系的网格分得足够细密(也就是每个网格变得充分小)。那么通过数圆内的的整点数目，你可以发现，这个数目大致和圆的面积差不多(实际上，直观的也可以看出这一点)。也就是说，$A(r)$ 大致就等于 πr。但是任何近似的估计如果不给出误差估计实际上是没有任何意义的，因此你看出来了 $A(r)$ 大致就等于 πr 还没有完，还必须无论如何也要定出一个 $|A(r)-\pi r|$ 的一个界限才使得你的估计能有用。显然，这个误差的阶必须要小于 $Cr^{1-\epsilon}$ 才有意义，其中 C 是一个常数，否则就说明你那个 πr 还可以改进。现在我们就来给出一个这种误差估计。为此，先引进一个符号。

定义 3.8.4 设 $f(x)$ 是一个任意函数，而 $\varphi(x)$ 是一个函数值恒为正的函数，如果存在常数 C，使得对于充分大的 x 值，成立不等式 $|f(x)|\leqslant C\varphi(x)$，则说当 $x\to\infty$ 时

$$f(x) = C(\varphi(x))$$

定理 3.8.7 当 $r\to\infty$ 时，$|A(r)-\pi r|\leqslant(2\sqrt{2}\pi+1)\sqrt{r}$。

证明 首先我们令每个边长为单位的格点正方形和它的左下角的各点相对应，这样就建立了全体单位正方形和全体各点的一个 1—1 对应。因为 $A(r)$ 表示圆 $\Gamma: x^2+y^2=r^2$ 内部及边界上的格点数。因此 $A(r)$ 等于左下角在 Γ 内或 Γ 上的所有单位格点正方形的面积之和。由于这些单位格点正方形的左下角与原点之间的距离不会超过$\sqrt{r}$，而每一个单位格点正方形内任一点与左下角的距离不超过$\sqrt{2}$，因此任何一个左下角在 Γ 内或Γ 上的单位格点正方形内的

点与原点的距离不可能超过$\sqrt{r}+\sqrt{2}$。即所有左下角在Γ内或Γ上的单位格点正方形必包含在以原点为圆心，$\sqrt{r}+\sqrt{2}$为半径的圆内。故得

$$A(r) \leqslant \pi(\sqrt{r}+\sqrt{2})^2$$

另一方面，在以原点为圆心，以$\sqrt{r}-\sqrt{2}$为半径的圆上任取一点$P(x,y)$，那么以$Q([x],[y])$为左下角的单位格点正方形K显然覆盖了点P。而$OQ \leqslant OP+PQ \leqslant \sqrt{r}-\sqrt{2}+\sqrt{2} \leqslant \sqrt{r}$，因此$K$是一个左下角在$\Gamma$内或$\Gamma$上的单位格点正方形。由于点$P$的任意性，就知道全体左下角在$\Gamma$内或$\Gamma$上的单位格点正方形必然覆盖了以原点为圆心，$\sqrt{r}-\sqrt{2}$以为半径的圆。因此又有

$$\pi(\sqrt{r}-\sqrt{2})^2 \leqslant A(r)$$

由上面两个不等式即得

$$\pi(-2\sqrt{2}\sqrt{r}+2) \leqslant A(r)-\pi r \leqslant \pi(2\sqrt{2}\sqrt{r}+2)$$

或
$$|A(r)-\pi r| \leqslant \pi(2\sqrt{2}\sqrt{r}+2)$$

当$r \geqslant 4\pi^2$时，$2\pi \leqslant \sqrt{r}$，因此上式就成为

$$|A(r)-\pi r| \leqslant (2\sqrt{2}\pi+1)\sqrt{r}$$

这就证明了定理。

由上面的定理显然即可推出$A=\pi r+O(\sqrt{r})$。

设α满足条件$A(r)=\pi r+O(r^{\alpha})$，那么可以证明$\alpha \geqslant \frac{1}{4}$。因此所有满足条件$A(r)=\pi r+O(r^{\alpha})$的数$\alpha$必有一个最小的下界$\vartheta$，称为所有$\alpha$的下确界（这是数学分析中已经证明过的一条基本定理）。由定理3.8.7可知$\vartheta \leqslant \frac{1}{2}$。这个下确界的确切值究竟是多少就是著名的高斯圆内格点问题。至今仍未解决。目前大家都猜测$\vartheta=\frac{1}{4}$。我国数学家华罗庚证明了$\vartheta \leqslant \frac{13}{40}$。

圆这个东西，从外表上看起来和双曲线$x^2-y^2=1$，或双曲线$xy=1$（这两条曲线只不过在坐标系中的位置不一样，实质上的形状是一样的）很不一样，其实它们的方程只差了一个符号。所以有些和它们有关的事情其实很相像。比如如果把圆$x^2+y^2=1$换成双曲线$x^2-y^2=1$，然后也像定义三角函数那样也可以定义一些称为双曲函数的东西。如双曲正弦$\sinh x$，双曲余弦$\cosh x$，双曲正切$\tanh x$等等，并且可以证明，他们也满足一些和三角公式相类似的公式。例如

$$\cosh^2 x-\sinh^2 x=1$$

$$1-\tanh^2 x=\frac{1}{\cosh^2 x}$$

$$\sinh(x \pm y)=\sinh x\cosh y \pm \cosh x\sinh y$$

$$\cosh(x \pm y)=\cosh x\cosh y \pm \sinh x\sinh y$$

等等。

同样,如果把圆 $x^2+y^2=r^2$ 换成双曲线 $xy=r$,并且在第一象限中考虑它和两个坐标轴之间的格点数 $D(r)$,就得到所谓除数问题。对除数问题也有和圆内格点问题类似的一个误差估计

$$D(r)=r(\ln r+2r-1)+O(\sqrt{r})$$

同样也可以问,满足条件 $D(r)=r(\ln r+2\gamma-1)+O(r^{\alpha})$ 的所有 α 的下确界 υ 究竟是多少的问题。这一问题至今也没有解决。但是也和圆内格点问题一样可以证明 $\vartheta\geqslant\frac{1}{4}$。同样大家也都猜测 $\vartheta=\frac{1}{4}$。我国数学家迟宗陶应用闵嗣鹤的一种估计三角和的方法得到了 $\vartheta\leqslant\frac{15}{46}$。

定理 3.8.5 和定理 3.8.6 可以推广成为一般的形式,为此,我们需先引进贝努利(Bernoulli)数和贝努利多项式的概念。

定义 3.8.5 函数 $\frac{x}{e^x-1}$ 的展开式 $\sum\limits_{n=0}^{\infty}\frac{B_n}{n!}x^n$, $|x|<2\pi$ 中 x^n 的系数 $\frac{B_n}{n!}$ 中的数 B_n 称为第 n 个贝努利数。

通过计算可以得到前几个贝努利数为

$$B_0=1,B_1=-\frac{1}{2},B_2=\frac{1}{6},B_3=0,B_4=-\frac{1}{30}$$

$$B_5=0,B_6=-\frac{1}{42},B_7=0,B_8=-\frac{1}{30},B_9=0$$

除了能看出来在 $n\geqslant2$ 时有 $B_{2n-1}=0$,其他的似乎还看不出什么规律。下面给出贝努利多项式和贝努利数的一些性质。

定理 3.8.8 贝努利数有以下性质:

(1) $B_3=B_5=B_7=\cdots=B_{2k-1}=0,k\geqslant2$;

(2) B_n 满足递推关系:把 $(B+1)^{n+1}-B^{n+1}=0,n=1,2,3,\cdots$ 按照通常的二项式展开法则展开,消去最高次项后,再把方幂 B^k 换成 B_k。如此得到

$$\begin{aligned}&2B_1+1=0\\&3B_2+3B_1+1=0\\&4B_3+6B_2+4B_1+1=0\\&5B_4+10B_3+10B_2+5B_1+1=0\\&\vdots\end{aligned}$$

等等。

(3) $B_{2n}=(-1)^{n-1}\frac{2(2n)!}{(2\pi)^{2n}}\zeta(2n)$,其中 $\zeta(2n)=\sum\limits_{k=1}^{\infty}\frac{1}{k^{2n}}$。

证明 (1) 由于

$$\frac{x}{e^x-1}+\frac{x}{2}=\frac{x}{2}\frac{e^x+1}{e^x-1}=-\frac{xe^{-x}+1}{2e^{-x}-1}$$

所以我们知道$\frac{x}{e^x-1}+\frac{x}{2}$是一个偶函数，也就是说，$\frac{x}{e^x-1}+\frac{x}{2}$的展开式中所有奇次幂的系数都是0。而显然$\frac{x}{e^x-1}+\frac{x}{2}$的展开式与$\frac{x}{e^x-1}$的展开式对大于或者等于2次以上的幂是相同的。这就证明了

$$B_3=B_5=B_7=\cdots=B_{2k-1}=0,k\geqslant 2$$

(2) 从$\frac{x}{e^x-1}=\sum_{n=0}^{\infty}\frac{B_n}{n!}x^n$，$|x|<2\pi$得出

$$(e^x-1)\sum_{n=0}^{\infty}\frac{B_n}{n!}x^n=x$$

从而

$$\left(1+x+\frac{1}{2!}x^2+\cdots+\frac{1}{n!}x^n+\cdots-1\right)\sum_{n=0}^{\infty}\frac{B_n}{n!}x^n=x$$

$$\left(x+\frac{1}{2!}x^2+\cdots+\frac{1}{n!}x^n+\cdots\right)\sum_{n=0}^{\infty}\frac{B_n}{n!}x^n=x$$

$$\left(1+\frac{1}{2!}x+\cdots+\frac{1}{n!}x^{n-1}+\cdots\right)\left(1+\frac{B_1}{1!}x+\frac{B_2}{2!}x^2+\cdots+\frac{B_n}{n!}x^n+\cdots\right)=1$$

于是由级数的乘法法则，并比较等式两边同次幂的系数就得到

$$\frac{B_n}{n!1!}+\frac{B_{n-1}}{(n-1)!2!}+\cdots+\frac{B_{n-k+1}}{(n-k+1)!k!}+\cdots+\frac{B_1}{1!n!}+\frac{1}{(n+1)!}=0$$

在等式两边同乘以$(n+1)!$就得到

$$C_{n+1}^1B_n+C_{n+1}^2B_{n-1}+\cdots+C_{n+1}^kB_{n+1-k}+\cdots+C_{n+1}^nB_1+1=0$$

利用上面的式子与二项式的展开式的相似性就得到定理中所说的递推法则。

由以上递推关系式可以看出贝努利数全都是有理数。

(3) 回忆双曲函数的无穷乘积展开式

$$\sinh x=x\prod_{n=1}^{\infty}\left(1+\frac{x^2}{n^2\pi^2}\right),\cosh x=\prod_{n=1}^{\infty}\left(1+\frac{x^2}{\left(\frac{2n-1}{2n}\pi\right)^2}\right)$$

（见菲赫金哥尔茨《微积分学教程》第二卷第二分册413页例8)）。在$\sinh x$的无穷乘积展开式的两边取对数就得到

$$\ln(\sinh x)=\ln x+\sum_{n=1}^{\infty}\ln\left(1+\frac{x^2}{n^2\pi^2}\right)$$

对上式逐项微分得

$$\coth x=\frac{1}{x}+\sum_{n=1}^{\infty}\frac{2x}{x^2+n^2\pi^2}$$

菲赫金哥尔茨(Фихтенгольц, Григорий Михайлович, 1888—1959)，苏联数学家，生于敖德萨.

$$x\coth x = 1 + 2\sum_{n=1}^{\infty} \frac{x^2}{x^2 + n^2\pi^2}$$

把上式中的 x 换成 πx 就得到

$$\pi x\coth \pi x = 1 + 2\sum_{n=1}^{\infty} \frac{x^2}{n^2 + x^2}$$

现在设 $|x| < 1$,那么就有

$$\frac{x^2}{k^2 + x^2} = \frac{\frac{x^2}{k^2}}{1 - \frac{x^2}{k^2}} = \sum_{n=1}^{\infty}(-1)^{n-1}\left(\frac{x^2}{k^2}\right)^n$$

因此按照幂级数的运算法则

$$\sum_{k=1}^{\infty} \frac{x^2}{k^2 + x^2} = \sum_{n=1}^{\infty}(-1)^{n-1}\zeta(2n)x^{2n}$$

其中

$$\zeta(2n) = \sum_{k=1}^{\infty} \frac{1}{k^{2n}}, n = 1,2,3,\cdots$$

这样对于 $|x| < 1$ 就有

$$\pi x\coth \pi x = 1 + 2\sum_{n=1}^{\infty}(-1)^{n-1}\zeta(2n)x^{2n}, \ |x| < 1$$

另一方面把

$$\frac{x}{e^x - 1} + \frac{x}{2} = \frac{x}{2}\cdot\frac{e^x + 1}{e^x - 1} = \frac{x}{2}\coth\frac{x}{2}$$

式子中的 x 换成 $2x$,就得到

$$\frac{2x}{e^{2x} - 1} + x = x\coth x$$

$$x\coth x = 1 + \frac{2^2B_2}{2!}x^2 + \frac{2^4B_4}{4!}x^4 + \cdots + \frac{2^{2n}B_{2n}}{2n!}x^{2n} + \cdots = 1 + \sum_{n=1}^{\infty}\frac{2^{2n}B_{2n}}{2n!}x^{2n}$$

再把上式中的 x 换成 πx 就得到

$$\pi x\coth \pi x = 1 + \sum_{n=1}^{\infty}(-1)^{n-1}\frac{(-1)^{n-1}(2\pi)^{2n}B_{2n}}{2n!}x^{2n}$$

对比 $\pi x\coth \pi x$ 的两种表达式(它们当然必须相等)最后就得到

$$B_{2n} = (-1)^{n-1}\frac{2(2n)!}{(2\pi)^{2n}}\zeta(2n)$$

由于当 $n\to\infty$ 时,$\zeta(2n)\to 1$,故从上面的式子中可以看出,当 $n\to\infty$ 时,$|B_{2n}|\to\infty$。这恐怕是一开始想不到的。

下面我们再定义贝努利多项式的概念。

定义 3.8.6 $B_n(x) = \sum_{k=0}^{n} C_n^k B_k x^{n-k}$,称为第 n 个贝努利多项式。

定理 3.8.9 贝努利多项式有以下性质：

(1) $\frac{ye^{xy}}{e^y-1}=\sum_{n=0}^{\infty}\frac{B_n(x)}{n!}y^n$;

(2) $B_n(1+x)-B_n(x)=nx^{n-1}$;

(3) $B_n(1-x)=(-1)^nB_n(x)$;

(4) $B'_n(x)=nB_{n-1}(x)$;

(5) 当 $n\geqslant 2$ 时，$B_n(0)=B_n(1)$。

证明 (1) 设$\frac{y}{e^y-1}e^{xy}$ 的展开式中，y^n 前的系数是$\frac{W_n(x)}{n!}$，则我们有恒等式

$$\sum_{n=0}^{\infty}\frac{W_n(x)}{n!}y^n=\frac{y}{e^y-1}e^{xy}=\Big(\sum_{n=0}^{\infty}\frac{B_n}{n!}y^n\Big)\Big(\sum_{n=0}^{\infty}\frac{x^n}{n!}y^n\Big)$$

比较等式两边 y^n 前的系数就得到

$$W_n(x)=\sum_{k=0}^{n}C_n^kB_kx^{n-k}=B_n(x)$$

(2) 我们有恒等式$\frac{ye^{(x+1)y}}{e^y-1}-\frac{ye^{xy}}{e^y-1}=ye^{xy}$，由此得到

$$\sum_{n=0}^{\infty}\frac{B_n(x+1)-B_n(x)}{n!}y^n=\sum_{n=0}^{\infty}\frac{x^n}{n!}y^{n+1}$$

比较上式中 y^n 前的系数就证明了定理的第(2) 部分。

(3) 我们有恒等式

$$\frac{-ye^{-xy}}{e^{-y}-1}=\frac{-ye^{-xy}e^y}{1-e^y}=\frac{ye^{(1-x)y}}{e^y-1}$$

由此得到

$$\sum_{n=0}^{\infty}\frac{(-1)^nB_n(x)}{n!}y^n=\sum_{n=0}^{\infty}\frac{B_n(1-x)}{n!}y^n$$

比较上式中 y^n 前的系数就证明了定理的第(3) 部分。

(4) $B'_n(x)=\sum_{k=0}^{n}C_n^kB_k(n-k)x^{n-k-1}=\sum_{k=0}^{n-1}nC_{n-1}^kB_kx^{n-1-k}=nB_{n-1}(x)$;

(5) 在(2) 中令 $x=0$ 即得。

利用以上性质，我们可以计算出开头几个贝努利多项式如下

$$B_1(x)=x-\frac{1}{2},B_2(x)=\frac{1}{2}x^2-\frac{1}{2}x+\frac{1}{12}$$

$$B_3(x)=\frac{1}{6}x^3-\frac{1}{4}x^2+\frac{1}{12}x,B_4(x)=\frac{1}{24}x^4-\frac{1}{12}x^3$$

利用上面定理中的性质(4) 和分部积分法则，当 $n\geqslant 1$ 时，我们可进行如下的分部积分

$$\frac{1}{m!}\int_1^n B_m(\{x\})f^{(m)}(x)\mathrm{d}x = \frac{1}{(m+1)!}(B_{m+1}(1)f^{(m)}(n) - B_{m+1}(0)f^{(m)}(1)) - \frac{1}{(m+1)!}\int_1^n B_{m+1}(\{x\})f^{(m+1)}(x)\mathrm{d}x$$

利用上面的公式，在定理3.8.5或定理3.8.6中连续地进行分部积分，即可得到下面的一般的求和公式。

马克劳林（Maclaurin，Colin，1698—1746），英国数学家，生于苏格兰基尔莫丹，卒于爱丁堡。

定理3.8.10（欧拉 - 马克劳林求和公式）

$$\sum_{1\leqslant k<n} f(k) = \int_1^n f(x)\mathrm{d}x - \frac{1}{2}(f(n) - f(1)) + \frac{1}{2!}(B_2(1)f'(n) - B_2(0)f'(1)) + \cdots + \frac{(-1)^m}{m!}(B_m(1)f^{(m-1)}(n) - B_m(0)f^{(m-1)}(1)) + R_m = \int_1^n f(x)\mathrm{d}x + \sum_{k=1}^{m}\frac{(-1)^k B_k}{k!}(f^{(k-1)}(n) - f^{(k-1)}(1)) + R_m$$

其中

$$R_m = \frac{(-1)^{m+1}}{m!}\int_1^n B_m(\{x\})f^{(m)}(x)\mathrm{d}x$$

当$\frac{B_m(\{x\})}{m!}f^{(m)}(x)$非常小时，余项$R_m$也将很小。而且事实上，已知当$m$是偶数时，$|B_m(\{x\})|\leqslant|B_m|$，并且$\left|\frac{B_m(\{x\})}{m!}\right| < \frac{4}{(2\pi)^m}$。另一方面，通常得出的结果是，当$m$增大时，$f^{(m)}(x)$也随之变大，所以$m$有一个使$R_m$取最小值的"最好"的值。

如果当x从1增加到n时，$f^{(2k+1)}(x)$和$f^{(2k+3)}(x)$单调地趋于0，则已经知道

$$R_{2k} = \frac{B_{2k+2}}{(2k+2)!}(f^{(2k+1)}(n) - f^{(2k+1)}(0))\theta, 0<\theta<1 \qquad (*)$$

（所以在这种情况下，余项与第一个被删去的项同号，而且小于这一项）。

现在我们来举一个应用欧拉 - 马克劳林公式的例子。设$f(x) = \frac{1}{x}$，那么

$$f^{(m)}(x) = \frac{(-1)^m m!}{x^{m+1}}$$

所以由欧拉 - 马克劳林公式就得到

$$H_{n-1} = \ln n + \sum_{k=1}^{m}\frac{B_k}{k}(-1)^{k-1}\left(\frac{1}{n^k} - 1\right) + R_{mn}$$

由无穷积分收敛性的判断法则得知下列极限的存在性

$$\lim_{n\to\infty} R_{mn} = -\int_1^{\infty}\frac{B_m(\{x\})}{x^{m+1}}\mathrm{d}x$$

这就顺便证明了所谓欧拉常数的存在性

$$\gamma = \lim_{n\to\infty}(H_{n-1} - \ln n) = \sum_{k=1}^{m} \frac{B_k}{k}(-1)^k + \lim_{n\to\infty} R_{mn}$$

于是就得到

$$H_{n-1} = \ln n + \gamma + \sum_{k=1}^{m} \frac{(-1)^{k-1}B_k}{kn^k} + \int_n^{\infty} \frac{B_m(\{x\})}{x^{m+1}}\mathrm{d}x$$

进一步,根据误差估计式(*),误差小于删去的头一项,两边都加上$\frac{1}{n}$就得到

$$H_n = \ln n + \gamma + \frac{1}{2n} - \frac{1}{12n^2} + \frac{1}{120n^4} - \epsilon, 0 < \epsilon < \frac{B_6}{6n^6} = \frac{1}{252n^6}$$

对于大的 k 值,贝努利数 B_k 也非常大,因此对于任何固定的 n 值,上面的式子不可能扩充为一个收敛的无穷级数。

戴德金(Dedekind, Julius Wilhelm Richard, 1831—1916),德国数学家.生于德国不伦瑞克,卒于同地.

下面我们要介绍的是一个称为戴德金和的函数。为此先给出一个符号 $((x))$ 的意义。

定义 3.8.7 符号$((x))$ 的意义如下:

$$((x)) = \begin{cases} x - [x] - \frac{1}{2}, \text{如果 } x \text{ 不是整数} \\ 0, \text{如果 } x \text{ 是整数} \end{cases}$$

从定义可以看出,当 x 不是整数时,$((x))$ 的值就是 $B_1(\{x\})$。首先,我们给出一个有关$((x))$ 的性质的引理。

引理 3.8.3 $((x))$ 有以下性质:

(1) $((x))$ 是周期为 1 的周期函数;

(2) $((-x)) = -((x))$;

(3) 设$(h,k) = 1$,则

$$\sum_{r=0}^{k-1}\left(\left(\frac{hr}{k}\right)\right) = \sum_{r=0}^{k-1}\left(\left(\frac{r}{k}\right)\right) = 0$$

证明 (1) 当 x 不是整数时,由于

$$x + 1 - [x+1] = x + 1 - ([x] + 1) = x - [x]$$

因此由$((x))$的定义就得出$((x+1)) = ((x))$,当 x 是整数时,由$((x))$的定义就得出

$$((x+1)) = ((x)) = 0$$

综合这两种情况就证明了(1)。

(2) 由引理 3.8.1(2) 得出,当 x 不是整数时

$$((-x)) = -x - [-x] = -x - (-[x] - 1) = -x + [x] + 1$$

因此由$((x))$的定义就得出$((-x)) = -((x))$,当 x 是整数时,由$((x))$的定义就得出$((-x)) = 0 = -((x))$。综合这两种情况就证明了(2)。

(3) 由定理 3.7.2 即得

$$\sum_{r=0}^{k-1}\left(\left(\frac{hr}{k}\right)\right)=\sum_{r=0}^{k-1}\left(\left(\frac{r}{k}\right)\right)=0+\sum_{r=1}^{k-1}\left(\frac{r}{k}-0-\frac{1}{2}\right)=\frac{(k-1)k}{2k}-\frac{k-1}{2}=0$$

下面我们定义戴德金和。

定义 3.8.8 设 k 是正整数，$(h,k)=1$，则称 $s(h,k)=\sum_{r=0}^{k-1}\left(\left(\frac{r}{k}\right)\right)\left(\left(\frac{hr}{k}\right)\right)$ 为戴德金和。

关于戴德金和有以下初等性质：

引理 3.8.4

(1) $s(h,k)=\sum_{r=1}^{k-1}\frac{r}{k}\left(\frac{hr}{k}-\left[\frac{hr}{k}\right]-\frac{1}{2}\right)$；

(2) 如果 $h'\equiv\pm h\pmod{k}$，则 $s(h',k)=\pm s(h,k)$；

(3) 如果 $hh'\equiv\pm 1\pmod{k}$，则 $s(h',k)=\pm s(h,k)$；

(4) 如果 $h^2\equiv -1\pmod{k}$，则 $s(h,k)=0$。

证明 (1) 由引理 3.8.3(3) 得

$$\begin{aligned}s(h,k)=&\sum_{r=0}^{k-1}\left(\left(\frac{r}{k}\right)\right)\left(\left(\frac{hr}{k}\right)\right)=0+\sum_{r=1}^{k-1}\left(\left(\frac{r}{k}\right)\right)\left(\left(\frac{hr}{k}\right)\right)=\\&\sum_{r=1}^{k-1}\left(\frac{r}{k}-\left[\frac{r}{k}\right]-\frac{1}{2}\right)\left(\left(\frac{hr}{k}\right)\right)=\\&\sum_{r=1}^{k}\left(\frac{r}{k}\right)\left(\left(\frac{hr}{k}\right)\right)-\frac{1}{2}\sum_{r=1}^{k-1}\left(\left(\frac{hr}{k}\right)\right)=\\&\sum_{r=1}^{k-1}\left(\frac{r}{k}\right)\left(\left(\frac{hr}{k}\right)\right)=\sum_{r=1}^{k-1}\left(\frac{r}{k}\right)\left(\frac{hr}{k}-\left[\frac{hr}{k}\right]-\frac{1}{2}\right)\end{aligned}$$

(2)
$$\begin{aligned}s(h',k)=&\sum_{r=0}^{k-1}\left(\left(\frac{r}{k}\right)\right)\left(\left(\frac{h'r}{k}\right)\right)=\sum_{r=0}^{k-1}\left(\left(\frac{r}{k}\right)\right)\left(\left(\frac{\pm hr}{k}\right)\right)=\\&\pm\sum_{r=0}^{k-1}\left(\left(\frac{r}{k}\right)\right)\left(\left(\frac{hr}{k}\right)\right)=\pm s(h,k)\end{aligned}$$

(3) 由定理 3.7.2 即得

$$\begin{aligned}s(h',k)=&\sum_{r=0}^{k-1}\left(\left(\frac{r}{k}\right)\right)\left(\left(\frac{h'r}{k}\right)\right)=\sum_{r=0}^{k-1}\left(\left(\frac{r}{k}\right)\right)\left(\left(\frac{h'hr}{k}\right)\right)=\\&\sum_{r=0}^{k-1}\left(\left(\frac{r}{k}\right)\right)\left(\left(\frac{\pm r}{k}\right)\right)=\pm s(h,k)\end{aligned}$$

(4) 在(2) 中取 $h'=h$ 即得 $s(h,k)=-s(h,k)$，故 $s(h,k)=0$。

引理 3.8.4(1) 中的公式可用来对小的 h 计算 $s(h,k)$，例如

$$s(1,k)=\sum_{r=1}^{k-1}\frac{r}{k}\left(\frac{r}{k}-\frac{1}{2}\right)=\frac{(k-1)(k-2)}{12k}$$

$$s(2,k)=\sum_{r=1}^{k-1}\frac{r}{k}\left(\frac{2r}{k}-\left[\frac{2r}{k}\right]-\frac{1}{2}\right)=$$

$$\sum_{r=1}^{k-1}\left(\frac{2r}{k}-\frac{1}{2}\right)-\sum_{2r<k}\frac{r}{k}\left[\frac{2r}{k}\right]-\sum_{k<2r<2k}\frac{r}{k}\left[\frac{2r}{k}\right]=$$

$$\sum_{r=1}^{k-1}\frac{r}{k}\left(\frac{2r}{k}-\frac{1}{2}\right)-\sum_{k<2r<2k}\frac{r}{k}=\frac{(k-1)(k-5)}{24k},2\nmid k$$

戴德金和有一个与定理 3.8.4 类似的对称性的结果如下：

定理 3.8.11 设 $h>0,k>0,(h,k)=1$，则

$$s(h,k)+s(k,h)=\frac{h^2+k^2-3hk+1}{12hk}$$

证明 首先，我们有

$$\sum_{r=0}^{k-1}\left(\left(\frac{hr}{k}\right)\right)^2=\sum_{r=1}^{k-1}\left(\left(\frac{r}{k}\right)\right)^2=\sum_{r=1}^{k-1}\left(\frac{r}{k}-\frac{1}{2}\right)^2=$$

$$\frac{1}{k^2}\sum_{r=1}^{k-1}r^2-\frac{1}{k}\sum_{r=1}^{k-1}r+\frac{k-1}{4}$$

另一方面，我们又有

$$\sum_{r=0}^{k-1}\left(\left(\frac{hr}{k}\right)\right)^2=\sum_{r=1}^{k-1}\left(\frac{hr}{k}-\left[\frac{hr}{k}\right]-\frac{1}{2}\right)^2=$$

$$\sum_{r=1}^{k-1}\left(\frac{h^2r^2}{k^2}+\left[\frac{hr}{k}\right]^2+\frac{1}{4}-\frac{hr}{k}+\left[\frac{hr}{k}\right]-\frac{2hr}{k}\left[\frac{hr}{k}\right]\right)=$$

$$2h\sum_{r=1}^{k-1}\frac{r}{k}\left(\frac{hr}{k}-\left[\frac{hr}{k}\right]-\frac{1}{2}\right)+I-\frac{h^2}{k^2}\sum_{r=1}^{k-1}r^2+\frac{k-1}{4}$$

其中

$$I=\sum_{r=1}^{k-1}\left[\frac{hr}{k}\right]\left(\left[\frac{hr}{k}\right]+1\right)$$

利用引理 3.8.4(1) 中的公式并比较上面两个式子就得到

$$2hs(h,k)+I=\frac{(h^2+1)(k-1)(2k-1)}{6k}-\frac{k-1}{2} \qquad ①$$

由于 $0<r<k$，因此 $0<\frac{hr}{k}<h$，也就是说 $\left[\frac{hr}{k}\right]$ 只可能取 $0,1,2,\cdots,h-1$ 这 h 个值，或者 $\left[\frac{hr}{k}\right]=s-1,s=1,2,\cdots,h$。对给定的 s，设 $N(s)$ 表示 I 的和式中使得 $\left[\frac{hr}{k}\right]=s-1$ 的项的个数。$\left[\frac{hr}{k}\right]=s-1$ 的充分必要条件是 $s-1<\frac{hr}{k}<s$，或者 $\frac{k(s-1)}{h}<r<\frac{ks}{h}$。由于 $(h,k)=1$，所以 $r=\frac{k(s-1)}{h}$ 或者 $r=\frac{ks}{h}$ 的情况都是不可能发生的（否则将有 $(h,k)=k>1$，与假设矛盾）。因此对区间 $1\leqslant s\leqslant h-1$ 中的 s，只有从 $\left[\frac{k(s-1)}{h}\right]+1$ 到 $\left[\frac{ks}{h}\right]$ 的整数才能使得等式 $\left[\frac{hr}{k}\right]=s-1$ 成立，这就得出

$$N(s)=\left[\frac{ks}{n}\right]-\left[\frac{k(s-1)}{h}\right]$$

然而上面这个公式不适用于 $s=h$ 时的情况，因为这时，我们在计算使用的等式 $\left[\frac{hr}{k}\right]=s-1$ 成立的 r 的个数时必须去掉 $s=h$ 的情况，否则将有 $r=k$，而我们只对 0 至 $k-1$ 中的 r 求和。因此当 $s=h$ 时，上述公式成为

$$N(h)=k-1-\left[\frac{k(s-1)}{h}\right]$$

现在我们对 I 的求和公式作变量替换，即不再把 r 作为求和的脚标，而按照使得 $\left[\frac{hr}{k}\right]=s-1$ 的项的个数来重新排列和式中原来的项。说得再清楚些就是在 I 中把所有使得 $\left[\frac{hr}{k}\right]=0$ 的项收集在一起（这种项共有 $N(1)$ 个，而在 I 中它们的值是 $\left[\frac{hr}{k}\right]\left(\left[\frac{hr}{k}\right]+1\right)=0.1$），再把所有使得 $\left[\frac{hr}{k}\right]=1$ 的项收集在一起（这种项共有 $N(2)$ 个，而在 I 中它们的值是 $\left[\frac{hr}{k}\right]\left(\left[\frac{hr}{k}\right]+1\right)=1\cdot 2$）…… 最后再把所有使得 $\left[\frac{hr}{k}\right]=h-1$ 的项收集在一起（这种项共有 $N(h)$ 个，而在 I 中它们的值是 $\left[\frac{hr}{k}\right]\left(\left[\frac{hr}{k}\right]+1\right)=(h-1)\cdot h$），这样，我们就可以把 I 重新写成

$$\begin{aligned}I=&\sum_{s=1}^{h}(s-1)sN(s)=\sum_{s=1}^{h-1}(s-1)sN(s)+(h-1)hN(h)=\\&\sum_{s=1}^{h-1}(s-1)s\left(\left[\frac{ks}{h}\right]-\left[\frac{k(s-1)}{h}\right]\right)+(h-1)h\left(k-1-\left[\frac{k(h-1)}{h}\right]\right)=\\&\sum_{s=1}^{h-1}(s-1)s\left(\left[\frac{ks}{h}\right]-\left[\frac{k(s-1)}{h}\right]\right)+\\&(h-1)h\left(\left[\frac{hk}{h}\right]-\left[\frac{k(h-1)}{h}\right]\right)-h(h-1)=\\&\sum_{s=1}^{h}(s-1)s\left(\left[\frac{ks}{h}\right]-\left[\frac{k(s-1)}{h}\right]\right)-(h-1)h\end{aligned}$$

把最后得出的和式展开，你可以发现其中有些项是可以消去的，把这些项消去后再合并同类项就得到

$$I=-2\sum_{s=1}^{h-1}s\left[\frac{sk}{h}\right]+k(k-1)(h-1) \qquad ②$$

另一方面

$$\begin{aligned}2hs(k,h)=&2h\sum_{s=1}^{h-1}\frac{s}{h}\left(\frac{ks}{h}-\left[\frac{ks}{h}\right]-\frac{1}{2}\right)=2\sum_{s=1}^{h-1}s\left(\frac{ks}{h}-\left[\frac{ks}{h}\right]-\frac{1}{2}\right)=\\&-2\sum_{s=1}^{h-1}s\left[\frac{ks}{h}\right]+\frac{2k}{h}\sum_{s=1}^{h-1}s^2-\sum_{s=1}^{h-1}s\end{aligned}$$

因此 $$-2\sum_{s=1}^{h-1} s\left[\frac{ks}{h}\right] = 2hs(k,h) - \frac{2k}{h}\sum_{s=1}^{h-1} s^2 + \sum_{s=1}^{h-1} s$$

把上面的式子代入 ① 中就得到

$$I = 2hs(k,h) - \frac{2k}{h}\sum_{s=1}^{h-1} s^2 + \sum_{s=1}^{h-1} s + h(h-1)(k-1)$$

再把 I 的这一表达式代入 ① 中最后就得到

$$2hs(h,k) + 2hs(k,h) - \frac{2k}{h}\sum_{s=1}^{h-1} s^2 + \sum_{s=1}^{h-1} s + h(h-1)(k-1) = \frac{(h^2+1)(k-1)(2k-1)}{6k} - \frac{k-1}{2}$$

把上式中的两个和式算出来并在两边都乘以 $6k$，合并同类项就得到定理所要证明的公式。

戴德金和还有许多有趣的性质，这里就不介绍了，有兴趣的读者可以参看 TomM. Apostol 写的《Modular Functions and Dirichlet Series in Number Theory》一书。

例 3.8.4 设 a,b 是正整数，$a \mid b^2+1, b \mid a^2+1$，证明：

(1) $(a,b)=1$；

(2) $a^2+b^2+1=3ab$；

(3) $\frac{a^2+1}{b}=3a-b, \frac{b^2+1}{a}=3b-a$；

(4) 满足条件的所有正整数为 (F_{2n-1},F_{2n+1})，其中 F_n 表第 n 个斐波那契数。

证明 (1) 由已知条件可设 $a^2+1=bc, b^2+1=ad$，因此有

$$bc-a^2=1, ad-b^2=1$$

由这两个式子中的任何一个即得 $(a,b)=1$。

(2) 由 $a^2+1=bc, b^2+1=ad$ 知 $c \mid a^2+1$。

下面我们证明 $a \mid c^2+1$，实际上

$$(a^2+1)^2 = b^2c^2 = c^2(ad-1) = adc^2 - c^2$$

因此

$$c^2+1 = adc^2 - a^4 - 2a^2$$

这就证明了 $a \mid c^2+1$。

对 $a+b$ 施行数学归纳法。当 $a+b=1$ 时，$a=b=1$。故要证的等式显然成立。

假设对符合条件 $x \mid y^2+1, y \mid x^2+1, x+y \leqslant a+b$ 的正整数都成立等式 $a^2+b^2+1=3ab$，那么由于当 $b>1$ 时，$a \neq b$，由于 a,b 的地位是对称的，因此不妨设 $a \leqslant b$，从而 $a \leqslant b-1$，故

$$c=\frac{a^2+1}{b}<\frac{(a+1)^2}{b}\leqslant\frac{b^2}{b}\leqslant b$$

由此得出 $c\mid a^2+1,a\mid c^2+1$,且 $a+c<a+b$。因此由归纳法假设有 $c^2+a^2+1=3ca$。从而有

$$(a^2+1)^2=b^2c^2=b^2(3ac-a^2-1)=3acb^2-(a^2+1)b^2$$

由此得出

$$(a^2+1)(a^2+b^2+1)=3acb^2=3ab(a^2+1)$$

两边约去 a^2+1(它显然不等于0)后即得 $a^2+b^2+1=3ab$。因此由数学归纳法就证明了要证的等式。

(3) 由(2)已证的公式即可得出(3)中的式子。

(4) 由(2)中的证明过程可以看出如果设 $a^2+1=bc,b^2+1=ad$,那么数对(c,a)和(a,b)具有同样的性质,但是 $c+a<a+b$。因此可以通过变换 $T(a,b)=(c,a)$,其中 $c=\frac{a^2+1}{b}=3a-b$,把(a,b)连续的变换为一些新的数对$(a_{n-1},b_{n-1}),(a_{n-2},b_{n-2}),\cdots,(a_1,b_1)$。在此过程中 $a+b$ 的值每一次都将严格减小,因此必通过有限步就变为最小值2。这时 $a_1=b_1=1$,即 $T^n(a,b)=(1,1)$,因此 $T^{-n}(1,1),n=1,2,3,\cdots$ 就给出了全部符合要求的数对。

由 $T\begin{pmatrix}a\\b\end{pmatrix}=\begin{pmatrix}3a-b\\a\end{pmatrix}$可求出$T^{-1}\begin{pmatrix}a\\b\end{pmatrix}=\begin{pmatrix}b\\3b-a\end{pmatrix}$,因此

$$T^{-1}(1,1)=(1,2)=(F_1,F_3)$$

$$T^{-2}(1,1)=T^{-1}(1,2)=(2,5)=(F_3,F_5)$$

$$T^{-2}(1,1)=T^{-1}(2,5)=(5,13)=(F_3,F_7)$$

$$\vdots$$

因此我们有理由猜想 $T^{-n}(1,1)=(F_{2n-1},F_{2n+1})$,假设这一猜想成立,那么

$$\begin{aligned}T^{-(n+1)}(1,1)=T^{-1}T^{-n}(1,1)=T^{-1}(F_{2n-1},F_{2n+1})&=\\(F_{2n+1},3F_{2n+1}-F_{2n-1})&=\\(F_{2n+1},2F_{2n+1}+F_{2n}+F_{2n-1}-F_{2n-1})&=\\(F_{2n+1},F_{2n+1}+F_{2n+1}+F_{2n})&=\\(F_{2n+1},F_{2n+1})&\end{aligned}$$

因而由数学归纳法就证明了我们的猜想,这就给出了全部符合要求的数对。

在(2)中我们虽然用数学归纳法证明了公式 $a^2+b^2+1=3ab$,但是却没有说明这个公式是如何看出来的。我们指出,利用戴德金和的概念和前面的引理3.8.4和定理3.8.11可以立刻看出这个式子来。事实上,由条件中的 $a\mid b^2+1$, $b\mid a^2+1$ 和$(a,b)=1$立刻得出

$$a^2\equiv-1(\mathrm{mod}\ b),b^2\equiv-1(\mathrm{mod}\ a),(a,b)=1$$

因此由引理3.8.4得出 $s(a,b)=0, s(b,a)=0$，再由定理3.8.11即得出 $a^2+b^2+1=3ab$。

$n!$也是一个重要的整数的函数，把它加以推广，可以得到所谓的 Γ - 函数。这也是一个非常重要的函数。但是限于篇幅，我们不在此详细讨论 Γ - 函数。有兴趣的读者可以参看非赫金哥尔茨著的《微积分学教程》等书。像 $n!$这种函数，我们经常需要用一些已知的函数和比较简单的公式来刻画他的增长速度和对于很大的 n 这些函数的主要部分。下面我们就来介绍这方面的结果。所得的结果本身细想起来也是很有意思的。原因在于，这些函数本来都是离散的，但是我们却能用一些连续的函数来逼近他们，而且这些逼近的函数在一开始简直难以猜想，等你知道结果后，往往会有不可思议之感。

首先给出以下引理。

引理 3.8.5 设 $J_m=\int_0^{\frac{\pi}{2}}\sin^m x\mathrm{d}x$，则

$$J_{2n}=\frac{(2n-1)(2n-3)\cdots3\cdot1}{2n(2n-2)\cdots4\cdot2}\cdot\frac{\pi}{2}$$

$$J_{2n+1}=\frac{2n(2n-1)\cdots4\cdot2}{(2n+1)(2n-1)\cdots3\cdot1}$$

证明 分步积分就得到

$$J_m=\int_0^{\frac{\pi}{2}}\sin^{m-1}x(-\cos x)'\mathrm{d}x=$$

$$-\sin^{m-1}x\cos x\Big|_0^{\frac{\pi}{2}}+(m-1)\int_0^{\frac{\pi}{2}}\sin^{m-2}x\cos^2x\mathrm{d}x$$

上面的式子中右端前面的一项显然为零，在后面一项中，用 $1-\sin^2x$ 代替 $\cos^2x$ 即得

$$J_m=(m-1)J_{m-2}-(m-1)J_m$$

由此得到迭代公式

$$J_m=\frac{m-1}{m}J_{m-2}$$

瓦利斯(Wallis, John, 1616—1703)，英国数学家．生于肖特郡阿什福德，卒于牛津．

按照上面的公式，J_m 最终化为计算 J_0 或 J_1，由此即可得到引理中的公式。

引理 3.8.6 瓦利斯公式

$$\frac{\pi}{2}=\lim_{n\to\infty}\left(\frac{2n!!}{(2n-1)!!}\right)^2\frac{1}{2n+1}=\lim_{n\to\infty}\frac{2\cdot2\cdot4\cdot4\cdot\cdots\cdot2n\cdot2n}{1\cdot3\cdot3\cdot5\cdot\cdots\cdot(2n-1)\cdot(2n+1)}$$

证明 $0<x<\frac{\pi}{2}$，则由 $0<\sin x<1$ 易证下面的不等式成立，即

$$\sin^{2n+1}x<\sin^{2n}x<\sin^{2n-1}x$$

从 0 到 $\frac{\pi}{2}$ 积分上述不等式并利用引理 3.8.5 便得到

$$\frac{2n!!}{(2n+1)!!} < \frac{(2n-1)!!}{2n!!}\frac{\pi}{2} < \frac{(2n-2)!!}{(2n-1)!!}$$

或者
$$\left(\frac{2n!!}{(2n-1)!!}\right)^2\frac{1}{2n+1} < \frac{\pi}{2} < \left(\frac{2n!!}{(2n-1)!!}\right)^2\frac{1}{2n}$$

上述不等式两端的差是

$$\frac{1}{2n(2n+1)}\left(\frac{2n!!}{(2n-1)!!}\right)^2 < \frac{1}{2n}\cdot\frac{\pi}{2}$$

因此当 $n\to\infty$ 时，上述不等式两端的差将趋于零，这就说明上述不等式的两端都将趋于它们的公共极限，即它们所夹的数 $\frac{\pi}{2}$，这就证明了引理。

定理 3.8.12 斯特林公式

斯特林(Stirling, James, 1692—1770)，英国数学家. 生于苏格兰的斯特灵郡，卒于爱丁堡.

$$n! = \sqrt{2\pi n}\left(\frac{n}{e}\right)e^{\frac{\theta}{12n}}, 0 < \theta < 1$$

证明 设 $|x|<1$，于是可把 $\ln(1+x)$ 展开为

$$\ln(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \cdots + (-1)^{n-1}\frac{x^n}{n} + \cdots$$

在上式中用 $-x$ 代替 x，并从原来的级数减去所得的级数就得到

$$\ln\frac{1+x}{1-x} = 2x\left(1 + \frac{x^2}{3} + \frac{x^4}{5} + \cdots + \frac{x^{2m}}{2m+1} + \cdots\right)$$

在上面的式子中取 $x = \frac{1}{2n+1}$，其中 n 是任意自然数，那么

$$\frac{1+x}{1-x} = \frac{n+1}{n}$$

把这些式子代入到上面的展开式中就得到

$$\ln\frac{n+1}{n} = \frac{2}{2n+1}\left(1 + \frac{1}{3}\cdot\frac{1}{(2n+1)^2} + \frac{1}{5}\cdot\frac{1}{(2n+1)^4} + \cdots\right)$$

或者
$$\left(n+\frac{1}{2}\right)\ln\left(1+\frac{1}{n}\right) = 1 + \frac{1}{3}\cdot\frac{1}{(2n+1)^2} + \frac{1}{5}\cdot\frac{1}{(2n+1)^4} + \cdots$$

上面的展开式显然大于 1 但是小于

$$1 + \frac{1}{3}\left(\frac{1}{(2n+1)^2} + \frac{1}{(2n+1)^4} + \cdots\right) = 1 + \frac{1}{12n(n+1)}$$

所以就得到

$$1 < \left(n+\frac{1}{2}\right)\ln\left(1+\frac{1}{n}\right) < 1 + \frac{1}{12n(n+1)}$$

$$e < \left(1+\frac{1}{n}\right)^{n+\frac{1}{2}} < e^{1+\frac{1}{12n(n+1)}}$$

令 $a_n = \frac{n!e^n}{n^{n+\frac{1}{2}}}$，则 $\frac{a_n}{a_{n+1}} = \frac{\left(1+\frac{1}{n}\right)^{n+\frac{1}{2}}}{e}$，因而从上面的不等式就得出

$$1 < \frac{a_n}{a_{n+1}} < e^{\frac{1}{12n(n+1)}} = \frac{e^{\frac{1}{12n}}}{e^{\frac{1}{12(n+1)}}}$$

由此得出

$$0 < \cdots < a_{n+1}e^{-\frac{1}{12(n+1)}} < a_n < \cdots < a_1$$

以及

$$a_n e^{-\frac{1}{12n}} < a_{n+1}e^{-\frac{1}{12(n+1)}} < a_n < a_1$$

这说明数列 a_n 递减而下方有界，因此必趋向于一个正的有限极限 $a > 0$，而数列 $a_n e^{-\frac{1}{12n}}$ 递增并显然趋于同一极限 a（由于 $e^{-\frac{1}{12n}} \to 1$）。这样我们就得到不等式

$$a_n e^{-\frac{1}{12n}} < a < a_n$$

令 $a_n = a \cdot e^{\frac{\theta}{12n}}$，则一方面 $e^{\frac{\theta}{12n}} = \frac{a_n}{a} > 1$，因此 $\theta > 0$，另一方面 $e^{\frac{\theta}{12n}-\frac{1}{12n}} = \frac{a_n e^{-\frac{1}{12n}}}{a} < 1$，因此 $\theta < 1$，合并这两个不等式就得到 $0 < \theta < 1$。

从 $a_n = ae^{\frac{\theta}{12n}}$ 和 a_n 的定义就得到

$$n! = a\sqrt{n}\left(\frac{n}{e}\right)^n e^{\frac{\theta}{12n}}, 0 < \theta < 1 \qquad ③$$

为了定出常数 a，我们应用恒等式

$$\frac{2n!!}{(2n-1)!!} = \frac{(2n!!)^2}{2n!} = \frac{2^{2n}(n!)^2}{2n!} \qquad ④$$

对 $2n!$ 应用式子 $n! = a\sqrt{n}\left(\frac{n}{e}\right)^n e^{\frac{\theta}{12n}}, 0 < \theta < 1$ 就得到

$$2n! = a\sqrt{2n}\left(\frac{2n}{e}\right)^{2n} e^{\frac{\varphi}{24n}}, 0 < \varphi < 1 \qquad ⑤$$

把 ③ ~ ⑤ 代入到瓦利斯公式中就得到

$$\frac{\pi}{2} = \lim_{n\to\infty} \frac{1}{2n+1} a^2 \frac{n}{2} e^{\frac{2\theta-\varphi}{12n}} = \frac{a^2}{4}$$

切比雪夫（Чебышев, пафнутий Львович, 1821—1894），俄国数学家、力学家。生于奥卡多沃，卒于彼得堡。

由此得出 $a = \sqrt{2\pi}$，把 a 的值代入到式子 $n! = a\sqrt{n}\left(\frac{n}{e}\right)^n e^{\frac{\theta}{12n}}, 0 < \theta < 1$ 中去，就证明了定理。

下面我们引进两个通常以切比雪夫命名的函数。

定义 3.8.9 切比雪夫函数的意义如下：

$$\theta(x) = \sum_{p \leqslant x} \ln p$$

$$\psi(x) = \sum_{p^m \leqslant x} \ln p$$

其中第二个和表示对所有本身及其方幂不超过 x 的素数求和。

例如，$\theta(12)=\ln 2+\ln 3+\ln 5+\ln 7+\ln 11$；由于 $2,2^2,2^3,3,3^2,5,7$ 和 11 都是方幂不超过 12 的素数，所以

$$\psi(12)=3\ln 2+2\ln 3+\ln 5+\ln 7+\ln 11$$

再比如

$$\psi(30)=4\ln 2+3\ln 3+2\ln 5+\ln 7+\ln 11+\ln 13+\ln 17+\ln 19+\ln 23+\ln 29=28.4765\cdots$$

引理 3.8.7 切比雪夫函数有以下性质

$$\psi(x)=\sum_{p\leqslant x}\left[\frac{\ln x}{\ln p}\right]\ln p$$

$$\psi(x)=\theta(x)+\theta(x^{\frac{1}{2}})+\theta(x^{\frac{1}{3}})+\theta(x^{\frac{1}{4}})+\cdots$$

证明 (1) 设素数 p 的不超过 x 的方幂共有 m 个，那么这些方幂就是 p，$p^2,\cdots,p^m$，按照 m 的定义，m 必须满足 $p^m\leqslant x<p^{m+1}$ 或者 $m\leqslant\frac{\ln x}{\ln p}<m+1$，由此就得出 $m=\left[\frac{\ln x}{\ln p}\right]$。于是按照 $\psi(x)$ 的定义就得出

$$\psi(x)=\sum_{p^m\leqslant x}\ln p=\sum_{p\leqslant x}m\ln p=\sum_{p\leqslant x}\left[\frac{\ln x}{\ln p}\right]\ln p$$

这就证明了引理的前半部分。

(2) 由集合的分解表达式

$$\{p\mid p^m\leqslant x\}=\bigcup_{k=1}^{m}\{p\mid p^k\leqslant x\}$$

我们就得到

$$\psi(x)=\sum_{p^m\leqslant x}\ln p=\sum_{p\leqslant x}\ln p+\sum_{p^2\leqslant x}\ln p+\cdots+\sum_{p^m\leqslant x}\ln p=\sum_{p\leqslant x}\ln p+\sum_{p\leqslant x^{\frac{1}{2}}}\ln p+\cdots+=\theta(x)+\theta(x^{\frac{1}{2}})+\cdots$$

这就证明了引理的后半部分。

现在我们利用切比雪夫函数给出前 n 个自然数的最小公倍数 d_n 的表达式。

定理 3.8.13 设 $d_n=[1,2,3,\cdots,n]$ 表示前 n 个自然数的最小公倍数，那么

$$\ln d_n=\psi(n)$$

证明 根据 d_n 的定义就有 $d_n=\prod_{p\leqslant n}p^{\alpha_p}$。其中 α_p 使得 $p^{\alpha_p}\leqslant n$，$p^{\alpha_p+1}>n$，因此 $\alpha_p=\left[\frac{\ln n}{\ln p}\right]$。于是我们就得到

$$\ln d_n=\ln\prod_{p\leqslant n}p^{\alpha_p}=\sum_{p\leqslant n}\alpha_p\ln p=\sum_{p\leqslant n}\left[\frac{\ln n}{\ln p}\right]\ln p=\psi(n)$$

为了给出后面的结果，我们需要先叙述下面的显而易见的原理。

恒等原理：设 $f(x)$ 和 $g(x)$ 都是对同一实数集合 D 有定义的只取整数值的函数。如果对任意 $u \in D$ 都有 $f(u) = g(u)$，那么我们就认为 $f(x)$ 和 $g(x)$ 在 D 上定义了一个相同的整数值函数，并记为 $f(x) = g(x)$（不管定义它们的公式或描述语言是否相同）。

我们用此原理来证明下面的引理。

引理 3.8.8　设 $T(x) = \ln([x]!)$，那么

$$T(x) = \psi(x) + \psi\left(\frac{x}{2}\right) + \psi\left(\frac{x}{3}\right) + \cdots$$

证明　设 x 是任意非负实数。p 是任意一个使得 $p \leqslant [x] < x$ 的素数。$\alpha(p,[x])$ 是在 $[x]!$ 的素因子分解式中 p 的指数。则由定理 3.8.2 知

$$\alpha(p,[x]) = \left[\frac{[x]}{p}\right] + \left[\frac{[x]}{p^2}\right] + \cdots + \left[\frac{[x]}{p^m}\right] = \alpha_1 + \alpha_2 + \cdots + \alpha_m$$

其中，m 使得 $p^m \leqslant [x] < p^{m+1}$。又设

$$W(x) = \psi(x) + \psi\left(\frac{x}{2}\right) + \psi\left(\frac{x}{3}\right) + \cdots$$

那么由引理 3.8.7 知，可把 $W(x)$ 排成如下的无限方阵

$$\begin{aligned} W(x) = {} & \theta(x) + \theta(x^{\frac{1}{2}}) + \theta(x^{\frac{1}{3}}) + \cdots + \\ & \theta\left(\frac{x}{2}\right) + \theta\left(\left(\frac{x}{2}\right)^{\frac{1}{2}}\right) + \theta\left(\left(\frac{x}{2}\right)^{\frac{1}{3}}\right) + \cdots + \\ & \theta\left(\frac{x}{i}\right) + \theta\left(\left(\frac{x}{i}\right)^{\frac{1}{2}}\right) + \theta\left(\left(\frac{x}{i}\right)^{\frac{1}{3}}\right) + \cdots + \cdots \end{aligned}$$

又设 p 在第一列中出现到 β_1 行，以后就不出现了，在第二列中出现到 β_2 行，以后就不出现了，…，在第 k 列中出现到 β_k 行，以后就不出现了，在第 $k+1$ 列中不出现。

首先证明 $k = m$。p 在第 k 列出现的充分必要条件是 p 在第一行第 k 列中出现。p 在第一行第 k 列中出现的充分必要条件是 $p \leqslant [x]^{\frac{1}{k}}$ 或者 $p^k \leqslant x$，因此由 $p^m \leqslant [x] < p^{m+1}$ 知 $m \leqslant k < m+1$，这就说明 $k = m$。

根据 β_j 的定义，p 在第 j 列中一直出现到第 β_j 行，而在 $\beta_j + 1$ 行中就不再出现。因此 β_j 必须满足条件 $p \leqslant \left(\frac{[x]}{\beta_j}\right)^{\frac{1}{j}}$，$p > \left(\frac{[x]}{\beta_j + 1}\right)^{\frac{1}{j}}$ 或者 $p^j \leqslant \frac{[x]}{\beta_j}$，$p^j > \frac{[x]}{\beta_j + 1}$，这也就是 $\beta_j \leqslant \frac{[x]}{p^j} < \beta_j + 1$，于是对照 α_j 的定义即可知道 $\alpha_j = \beta_j$。这就说明 p 在 $W(x)$ 中共出现 $\beta_1 + \beta_2 + \cdots + \beta_m = \alpha_1 + \alpha_2 + \cdots + \alpha_m = \alpha(p,[x])$ 次。所以 p 对函数 $T(x)$ 和 $W(x)$ 所贡献的值都是 $\alpha(p,[x])\ln p$。由于 p 的任意

性，这就证明了对任意 $x \geqslant 0$，$T(x)$ 和 $W(x)$ 所取的值都是相同的，于是根据恒等原理就得到 $T(x) = W(x)$。这就证明了引理。

由斯特林公式(定理 3.8.12) 我们又有以下的关于函数 $T(x)$ 的不等式。

引理 3.8.9

$$\left(n+\frac{1}{2}\right)\ln n - n + \frac{1}{2}\ln 2\pi < T(n) <$$
$$\left(n+\frac{1}{2}\right)\ln n - n + \frac{1}{2}\ln 2\pi + \frac{1}{12n}$$

证明 在 $T(n) = \ln n!$两边取对数，并利用斯特林公式即得。

现在我们再定义一个函数 $U(n)$，通过这个函数可以利用函数 $T(n)$ 的特性来得出函数 $\psi(n)$ 的性质。本来函数 $\psi(n)$ 是很难研究的，但是函数 $T(n)$ 却比较好研究，所以通过函数 $U(n)$ 就迂回地弄清了 $\psi(n)$ 的一些特性。这就是当年切比雪夫给我们指出的一条路线。

定义 3.8.10 函数 $U(n)$ 的含义为

$$U(n) = T(n) - T\left(\frac{n}{2}\right) - T\left(\frac{n}{3}\right) - T\left(\frac{n}{5}\right) + T\left(\frac{n}{6}\right) - T\left(\frac{n}{7}\right) + T\left(\frac{n}{70}\right) - T\left(\frac{n}{210}\right)$$

引理 3.8.10 当 $n \geqslant 2$ 时，$U(n) < cn$，其中

$$c = \frac{1}{2}\ln 2 + \frac{1}{3}\ln 3 + \frac{1}{5}\ln 5 - \frac{1}{6}\ln 6 + \frac{1}{7}\ln 7 - \frac{1}{70}\ln 70 + \frac{1}{210}\ln 210 =$$
$$0.978\,795\,482\,576\,39$$

证明 从引理 3.8.9，我们有以下不等式

$$\left(n+\frac{1}{2}\right)\ln n - n + \frac{1}{2}\ln 2\pi < T(n) <$$
$$\left(n+\frac{1}{2}\right)\ln n - n + \frac{1}{2}\ln 2\pi + \frac{1}{12\,n}$$
$$-\left(\frac{n}{2}+\frac{1}{2}\right)\ln\frac{n}{2} + \frac{n}{2} - \frac{1}{2}\ln 2\pi - \frac{1}{24n} < -T\left(\frac{n}{2}\right) <$$
$$-\left(\frac{n}{2}+\frac{1}{2}\right)\ln\frac{n}{2} + \frac{n}{2} - \frac{1}{2}\ln 2\pi$$
$$-\left(\frac{n}{3}+\frac{1}{2}\right)\ln\frac{n}{3} + \frac{n}{3} - \frac{1}{2}\ln 2\pi - \frac{1}{36n} < -T\left(\frac{n}{3}\right) <$$
$$-\left(\frac{n}{3}+\frac{1}{2}\right)\ln\frac{n}{3} + \frac{n}{3} - \frac{1}{2}\ln 2\pi$$
$$-\left(\frac{n}{5}+\frac{1}{2}\right)\ln\frac{n}{5} + \frac{n}{5} - \frac{1}{2}\ln 2\pi - \frac{1}{60n} < T\left(\frac{n}{5}\right) - <$$
$$-\left(\frac{n}{5}+\frac{1}{2}\right)\ln\frac{n}{5} + \frac{n}{5} - \frac{1}{2}\ln 2\pi$$
$$\left(\frac{n}{6}+\frac{1}{2}\right)\ln\frac{n}{6} - \frac{n}{6} + \frac{1}{2}\ln 2\pi < T\left(\frac{n}{6}\right) <$$

$$\left(\frac{n}{6}+\frac{1}{2}\right)\ln\frac{n}{6}-\frac{n}{6}+\frac{1}{2}\ln 2\pi+\frac{1}{72n}$$

$$-\left(\frac{n}{7}+\frac{1}{2}\right)\ln\frac{n}{7}+\frac{n}{7}-\frac{1}{2}\ln 2\pi-\frac{1}{84n} < T\left(\frac{n}{7}\right) <$$

$$-\left(\frac{n}{7}+\frac{1}{2}\right)\ln\frac{n}{7}+\frac{n}{7}-\frac{1}{2}\ln 2\pi$$

$$\left(\frac{n}{70}+\frac{1}{2}\right)\ln\frac{n}{70}-\frac{n}{70}+\frac{1}{2}\ln 2\pi < T\left(\frac{n}{70}\right) < \left(\frac{n}{70}+\frac{1}{2}\right)\ln\frac{n}{70}-\frac{n}{70}+\frac{1}{2}\ln 2\pi+\frac{1}{840}$$

$$-\left(\frac{n}{210}+\frac{1}{2}\right)\ln\frac{n}{210}+\frac{n}{210}-\frac{1}{2}\ln 2\pi-\frac{1}{2\,520n} < -T\left(\frac{n}{210}\right) <$$

$$-\left(\frac{n}{210}+\frac{1}{2}\right)\ln\frac{n}{210}+\frac{n}{210}-\frac{1}{2}\ln 2\pi$$

把以上不等式相加，我们就得到对 $n \geqslant 1$，不等式

$$cn-\ln n+\frac{1}{2}\ln 105-\ln 2\pi-\frac{31}{315} < U(n) <$$

$$cn-\ln n+\frac{1}{2}\ln 105-\ln 2\pi+\frac{31}{315}$$

成立。从上面这个不等式就得到，对 $n \geqslant 2$，不等式

$$U(n) < cn-\ln n+0.587\,515\,807\,082\,11\cdots < cn$$

成立。这就证明了引理。

不知道是否所有的读者都注意到了，本来在引理3.8.9中是有 $n\ln n$ 项的，但是在上面的引理中最后得到的不等式里却没有这种项了，这就是说，它们被抵消了。它们之所以会被抵消，原因就在于 $U(n)$ 的定义中那些 $T\left(\frac{n}{i}\right)$ 项连同它们的符号的巧妙组合。于是可能有人会问，这个组合是怎么想出来的呢。答案是这个组合来源于恒等式

$$1-\frac{1}{2}-\frac{1}{3}-\frac{1}{5}+\frac{1}{6}-\frac{1}{7}+\frac{1}{70}-\frac{1}{210}=0$$

切比雪夫当年使用的是另一个恒等式

$$1-\frac{1}{2}-\frac{1}{3}-\frac{1}{5}+\frac{1}{30}=0$$

引理 3.8.11 $\qquad \psi(n)-\psi\left(\frac{n}{10}\right) < U(n)$

证明 从引理3.8.8我们有以下等式

$$T(n)=\psi(n)+\psi\left(\frac{n}{2}\right)+\psi\left(\frac{n}{3}\right)+\psi\left(\frac{n}{4}\right)+\psi\left(\frac{n}{5}\right)+\psi\left(\frac{n}{6}\right)+\cdots$$

$$T\left(\frac{n}{2}\right)=0\cdot\psi(n)+\psi\left(\frac{n}{2}\right)+0\cdot\psi\left(\frac{n}{3}\right)+\psi\left(\frac{n}{4}\right)+0\cdot\psi\left(\frac{n}{5}\right)+\psi\left(\frac{n}{6}\right)+\cdots$$

$$T\left(\frac{n}{3}\right)=0\cdot\psi(n)+0\cdot\psi\left(\frac{n}{2}\right)+\psi\left(\frac{n}{3}\right)+0\cdot\psi\left(\frac{n}{4}\right)+0\cdot\psi\left(\frac{n}{5}\right)+\psi\left(\frac{n}{6}\right)+\cdots$$

⋮

因此，从上面这些式子中可以看出，在 $T(n),T\left(\frac{n}{2}\right),T\left(\frac{n}{3}\right),T\left(\frac{n}{5}\right),T\left(\frac{n}{6}\right)$，$T\left(\frac{n}{7}\right),T\left(\frac{n}{70}\right)$ 和 $T\left(\frac{n}{210}\right)$ 中用 $\psi\left(\frac{n}{i}\right)$ 表示的展开式中，$\psi\left(\frac{n}{i}\right)$ 的系数都是 0 或 1。并且在上面的这 8 个展开式中，$\psi\left(\frac{n}{i}\right)$ 的系数构成了 8 个周期分别为 1,2,3,5,6,7,70 和 210 的周期数列。

由于 1,2,3,5,6,7,70 和 210 的最小公倍数 [1,2,3,5,6,7,70,210] = 210，以及周期数列之和仍为周期数列，所以我们知道在 $U(n)$ 的展开式中，$\psi\left(\frac{n}{i}\right)$ 的系数构成了一个周期为 210 的周期数列。

通过虽然繁琐但并不复杂的计算，我们可以得到 $U(n)$ 的展开式中的开头 210 项如下

$$
\begin{aligned}
U(n) = & \left(\psi(n)-\psi\left(\frac{n}{10}\right)\right)+\left(\psi\left(\frac{n}{11}\right)+\psi\left(\frac{n}{13}\right)-\psi\left(\frac{n}{14}\right)-\psi\left(\frac{n}{15}\right)\right)+ \\
& \left(\psi\left(\frac{n}{17}\right)+\psi\left(\frac{n}{19}\right)-\psi\left(\frac{n}{20}\right)-\psi\left(\frac{n}{21}\right)\right)+\left(\psi\left(\frac{n}{23}\right)-\psi\left(\frac{n}{28}\right)\right)+ \\
& \left(\psi\left(\frac{n}{29}\right)-\psi\left(\frac{n}{30}\right)\right)+\left(\psi\left(\frac{n}{31}\right)-\psi\left(\frac{n}{35}\right)\right)+ \\
& \left(\psi\left(\frac{n}{37}\right)-\psi\left(\frac{n}{40}\right)\right)+\left(\psi\left(\frac{n}{41}\right)-\psi\left(\frac{n}{42}\right)\right)+\left(\psi\left(\frac{n}{43}\right)-\psi\left(\frac{n}{45}\right)\right)+ \\
& \left(\psi\left(\frac{n}{47}\right)-\psi\left(\frac{n}{50}\right)\right)+\left(\psi\left(\frac{n}{53}\right)-\psi\left(\frac{n}{56}\right)\right)+ \\
& \left(\psi\left(\frac{n}{59}\right)-\psi\left(\frac{n}{60}\right)\right)+\left(\psi\left(\frac{n}{61}\right)-\psi\left(\frac{n}{63}\right)\right)+ \\
& \left(\psi\left(\frac{n}{67}\right)-\psi\left(\frac{n}{70}\right)\right)+\left(\psi\left(\frac{n}{71}\right)+\psi\left(\frac{n}{73}\right)-\psi\left(\frac{n}{75}\right)+\psi\left(\frac{n}{79}\right)-\psi\left(\frac{n}{80}\right)+\right. \\
& \left.\psi\left(\frac{n}{83}\right)-\psi\left(\frac{n}{84}\right)+\psi\left(\frac{n}{89}\right)-\psi\left(\frac{n}{90}\right)+\psi\left(\frac{n}{97}\right)-\psi\left(\frac{n}{98}\right)-\psi\left(\frac{n}{100}\right)\right)+ \\
& \left(\psi\left(\frac{n}{101}\right)+\psi\left(\frac{n}{103}\right)-2\psi\left(\frac{n}{105}\right)\right)+\left(\psi\left(\frac{n}{107}\right)+\psi\left(\frac{n}{109}\right)-\psi\left(\frac{n}{110}\right)-\right. \\
& \left.\psi\left(\frac{n}{112}\right)\right)+\left(\psi\left(\frac{n}{113}\right)-\psi\left(\frac{n}{120}\right)\right)+\left(\psi\left(\frac{n}{121}\right)-\psi\left(\frac{n}{126}\right)\right)+\left(\psi\left(\frac{n}{127}\right)-\right. \\
& \left.\psi\left(\frac{n}{130}\right)\right)+\left(\psi\left(\frac{n}{131}\right)-\psi\left(\frac{n}{135}\right)\right)+\left(\psi\left(\frac{n}{137}\right)+\psi\left(\frac{n}{139}\right)-\psi\left(\frac{n}{140}\right)+\psi\left(\frac{n}{143}\right)-\right. \\
& \psi\left(\frac{n}{147}\right)+\psi\left(\frac{n}{149}\right)-\psi\left(\frac{n}{150}\right)+\psi\left(\frac{n}{151}\right)-\psi\left(\frac{n}{154}\right)+\psi\left(\frac{n}{157}\right)-\psi\left(\frac{n}{160}\right)+ \\
& \psi\left(\frac{n}{163}\right)-\psi\left(\frac{n}{165}\right)+\psi\left(\frac{n}{167}\right)-\psi\left(\frac{n}{168}\right)+\psi\left(\frac{n}{169}\right)-\psi\left(\frac{n}{170}\right)+\psi\left(\frac{n}{173}\right)-\psi\left(\frac{n}{175}\right)+
\end{aligned}
$$

$$\psi\left(\frac{n}{179}\right)-\psi\left(\frac{n}{180}\right)+\psi\left(\frac{n}{181}\right)-\psi\left(\frac{n}{182}\right)+\psi\left(\frac{n}{187}\right)-\psi\left(\frac{n}{189}\right)-$$
$$\psi\left(\frac{n}{190}\right)\Big)+\left(\psi\left(\frac{n}{191}\right)+\psi\left(\frac{n}{193}\right)-\psi\left(\frac{n}{195}\right)-\psi\left(\frac{n}{196}\right)\right)+$$
$$\left(\psi\left(\frac{n}{197}\right)+\psi\left(\frac{n}{199}\right)-\psi\left(\frac{n}{200}\right)+\psi\left(\frac{n}{209}\right)-2\psi\left(\frac{n}{210}\right)\right)+\cdots$$

从 $\psi(n)$ 的定义可知 $\psi(n)$ 是递增函数，因此 $T(n)=\psi(n)+\psi\left(\frac{n}{2}\right)+\psi\left(\frac{n}{3}\right)+\cdots$ 是一个有限级数。因此 $U(n)$ 也是一个有限级数。容易验证在上面式子中的每个括号中的和数是一个正数。这就意味着，把 $U(n)$ 经过适当的分组后(每 210 项分为一大组，每一个大组中的小组的分法与开头的 210 项类似。由于 $U(n)$ 是一个有限级数，所以这种分组是合法的)，可以把 $U(n)$ 表示成为一个正项级数(开头的 210 项之和是一些正数之和，由于系数的周期性和 $\psi(n)$ 的递增性，以后的每 210 项之和也是一个正数)，去掉第三项之后的项，就得到所需的不等式。

引理 3.8.12 当 $n\geqslant 1$ 时，$\psi(n)<\frac{10}{9}cn$。

证明 从引理 3.8.10 和引理 3.8.11 就得到当 $n\geqslant 2$ 时成立不等式

$$\psi(n)-\psi\left(\frac{n}{10}\right)<U(n)<cn$$

由此得出当 $n\geqslant 2$ 时成立不等式

$$\psi(n)<cn+\psi\left(\frac{n}{10}\right)$$

反复应用上述不等式就得到，并注意当 $10^k>n$ 时，$\psi\left(\frac{n}{10^k}\right)=0$，因此下式右端的级数是收敛的

$$\psi(n)<cn+\frac{cn}{10}+\frac{cn}{10^2}+\cdots<\frac{10}{9}cn$$

当 $n=1$ 时，通过直接验证可以知道上述不等式成立，这就证明了引理。

刚才我们提到，使用一个切比雪夫类型的恒等式(见引理 3.8.12 上面)可以在 3.8.10 中把 $n\ln n$ 类型的项消掉，于是就可以定义一个函数 $U(n)$。但是 $U(n)$ 还必须有另外一个性质，即它的展开式能够被表示成为一个正项级数，这个性质并不是每一个切比雪夫类型的恒等式可以自动带来的，而是必须通过试验才能发现的。例如，根据恒等式

$$1-\frac{1}{2}-\frac{1}{3}-\frac{1}{5}-\frac{1}{7}+\frac{1}{105}=0$$

你也可以定义一个函数 $U(n)$，但是这个函数的展开式却无法被表示成为一个

正项级数。

另外,我们可以证明$\frac{\psi(n)}{n}$的最大值是$\frac{\psi(113)}{113}$,然而这个结果却无法用这里这么简单和初等的方法得出来。

定理 3.8.14 设 $d_n=[1,2,3,\cdots,n]$表示前 n 个自然数的最小公倍数,那么当 $n\geqslant 1$ 时,成立不等式

$$d_n<3^n$$

证明 由上面证明的几个引理我们得出

$$d_n=e^{\psi(n)}<e^{\frac{10}{9}cn}\leqslant(e^{\frac{10}{9}c})^n\leqslant(2.966\ 997\ 611\ 231\ 59\cdots)^n<3^n$$

习题 3.8

1. 对$\sqrt{2}$和 1 实行辗转相除法如下:

$$\sqrt{2}=1\cdot 1+\sqrt{2}-1,0<\sqrt{2}-1<1$$
$$1=2\cdot(\sqrt{2}-1)+3-2\sqrt{2},0<3-2\sqrt{2}<\sqrt{2}-1$$
$$\sqrt{2}-1=2(3-2\sqrt{2})+5\sqrt{2}-7,0<5\sqrt{2}-7<3-2\sqrt{2}$$
$$\vdots$$

证明:这一算法不可能在有限步内结束。

2. 设 n 是任意正整数,α 是实数,证明:$[\alpha]+\left[\alpha+\frac{1}{n}\right]+\cdots+\left[\alpha+\frac{n-1}{n}\right]=[n\alpha]$。

3. 设 α,β 是任意二实数,证明:

(1) $[\alpha]-[\beta]=[\alpha-\beta]$或$[\alpha-\beta]+1$;

(2) $[2\alpha]+[2\beta]\geqslant[\alpha]+[\alpha+\beta]+[\beta]$。

4. 设 $r=\frac{4}{3}$,证明存在无穷多个正整数,使得$[nr]$是素数。

5. 求出一个自然数 n,使得在 $n!$中,素数 3 共出现了 7 次。

6. 证明:方程$[x]+[2x]+[4x]+[8x]+[16x]+[32x]=12\ 345$没有整数解。

7. 设 $\alpha=\frac{\sqrt{5}-1}{2}$,$n$ 是自然数,证明:$[r[rn]+r]+[r(n+1)]=n$。

8. 设 $\varphi=\frac{\sqrt{5}+1}{2}$,$\Delta_n=[[(n+1)\varphi]\varphi]-[[n\varphi]\varphi]$,证明:

(1) Δ_n 等于 2 或者 3;

(2) $[[(n+1)\varphi^2]\varphi]-[[n\varphi^2]\varphi]=2\Delta_n-1$;

(3) $[n\varphi]+[n\varphi^2]=[[n\varphi^2]\varphi]$;

(4) $[[n\varphi^2]\varphi]=[[n\varphi]\varphi^2]+1$。

9. 设 α 是正实数，n 是自然数。$a_n=[n(\alpha+1)]$，$b_n=\left[n\left(\frac{1}{\alpha}\right)+1\right]$，证明

$$\{a_n\}\cap\{b_n\}=\varnothing,\{a_n\}\cup\{b_n\}=\{1,2,3,\cdots,n\cdots\}$$

的充分必要条件是 α 是正无理数。

10. 设 α,β 是正实数，n 是自然数。$a_n=[n\alpha]$，$b_n=[n\beta]$，证明

$$\{a_n\}\cap\{b_n\}=\varnothing,\{a_n\}\cup\{b_n\}=\{1,2,3,\cdots,n\cdots\}$$

的充分必要条件是 α,β 是满足关系式 $\frac{1}{\alpha}+\frac{1}{\beta}=1$ 的正无理数。

11. 设 $m>0,(a,m)=1,b$ 是整数，证明：

(1) $\sum_{r=0}^{m-1}\left\{\frac{ar+b}{m}\right\}=\frac{1}{2}(m-1)$；

(2) $\sum_{(r,m)=1}\left\{\frac{ar}{m}\right\}=\frac{1}{2}\varphi(m)$。

12. (1) 设 $m>0,(a,m)=1,h\geqslant 0,c$ 是实数，$c\leqslant\psi(x)\leqslant c+h$，$S=\sum_{x=0}^{m-1}\left\{\frac{ax+\psi(x)}{m}\right\}$。

证明：$\left|S-\frac{1}{2}m\right|\leqslant h+\frac{1}{2}$。

(2) 设 M 是整数，$m>0,(a,m)=1$，A 和 B 都是实数，且

$$A=\frac{a}{m}+\frac{\lambda}{m^2},S=\sum_{x=M}^{M+m-1}\{Ax+B\}$$

证明：$\left|S-\frac{1}{2}m\right|\leqslant|\lambda|+\frac{1}{2}$。

(3) 设 M 是整数，$m>0,(a,m)=1$，函数 $f(x)$ 在区间 $M\leqslant x\leqslant M+m-1$ 中直到二阶的连续导数，且满足条件

$$f'(M)=\frac{a}{m}+\frac{\theta}{m^2},|\theta|<1,\frac{1}{A}\leqslant|f''(x)|\leqslant\frac{k}{A}$$

其中

$$1\leqslant m\leqslant\tau,\tau=A^{\frac{1}{3}},A\geqslant 2,k\geqslant 1$$

$$S=\sum_{x=M}^{M+m-1}\{f(x)\}$$

证明：$\left|S-\frac{1}{2}m\right|<\frac{k+3}{2}$。

13. (1) 设 $r>0$，T 是区域 $x^2+y^2\leqslant r^2$ 内的整点数，证明

$$T=1+4[r]+8\sum_{0<x\leqslant\frac{r}{\sqrt{2}}}[\sqrt{r^2-x^2}]-4\left[\frac{r}{\sqrt{2}}\right]^2$$

(2) 设 $n>0$，T 是区域 $x>0,y>0,xy\leqslant n$ 内的整点数，证明

$$T = 2\sum_{0<x<\sqrt{n}}\left[\frac{n}{x}\right] - [\sqrt{n}]^2$$

14. 设 n 是任一正整数，p 是一个素数，且 $n = a_0 + a_1 p + a_2 p^2 + \cdots, 0 \leqslant a_i < p$。证明：在 $n!$ 的素因子分解式中，素数 p 的方次数是

$$h = \frac{n - S_n}{p - 1}$$

其中，$S_n = a_0 + a_1 + a_2 + \cdots$。

3.9 同余式的方程

大多数人在刚接触同余式这个概念及其性质时都不会感到很难，因为这里面有很多形式上与等式类似的东西，所以我们会有似曾相识之感。所以既然可以从等式这个概念发展出方程式的概念，那么从同余式这个概念也可以发展出同余式的方程的一套理论也就不奇怪了。不过二者之间虽然有相似的地方，然而也有许多不同的地方，首先弄清楚它们的异同才能比较轻松地往前走，所以下面我们采取对照的方式介绍同余式方程的理论，对于与等式和方程的不同之处，我们用黑体字标出以引起注意。

等式和方程	同余式和同余式的方程
1. 对变量的所有可能的值都成立的等式称为恒等式。	1. 设同余式的模为 $m > 0$，对所有整数式成立的同余式称为是关于模 m 的恒等同余式 设 $f(x,y,z,\cdots)$ 是变量 $x,y,z,\cdots$ 的整多项式。如果 $f(x,y,z,\cdots)$ 中所有的系数都是 m 的倍数，则称 $f(x,y,z,\cdots) \equiv 0 \pmod{m}$ 是关于模 m 的绝对同余式
2. 仅对被称为是未知数的变量的某些值成立的等式称为是关于未知数的方程	2. 仅对被称为是未知数的变量的某些值成立的同余式称为条件同余式或同余式的方程
3. 未知数的使得方程两边相等的值称为方程的解	3. 条件同余式中的未知数的使得同余式两边同余的同余类称为同余式方程的解
4. 方程式中未知数的最高次项的次数称为同余式的次数	4. 条件同余式中未知数的最高次项的次数称为方程的次数
5. 方程式中未知数的个数称为方程式的元数	5. 条件同余式中未知数的个数称为同余式方程的元数

6.设给定了(1),(2) 两个方程,如果方程(1) 的解都是方程(2) 的解,并且反过来,方程(2) 的解也都是方程(1) 的解,则称方程(1),(2) 是互相同解的方程	6.设给定了(1),(2) 两个同余式,如果同余式(1) 的解都是同余式(2) 的解,并且反过来,同余式(2) 的解也都是同同余式(1) 的解,则称同余式(1),(2) 是互相同解的同余式
7.把方程式的两边和一个两边都是整式的等式的两边相加,所得的方程和原方程同解	7.把同余式的两边与恒等同余式或者绝对同余式的两边相加,所得的的同余式方程和原来的同余式方程同解
8.用一个不等于零的实数去乘以方程的两边,所得的方程和原方程同解	8.设同余式方程的模是 m,$(k,m)=1$,那么用整数 k 去乘同余式方程的两边所得的同余式方程和原同余式方程同解

显然,绝对同余式一定是恒等同余式,但是反过来,恒等同余式却不一定是绝对同余式。例如 $x(x+1)\equiv 0(\mathrm{mod}\ 2)$ 显然是一个恒等同余式(因为 x 和 $x+1$ 是两个连续的整数,其中必有一个是偶数),但是 $x(x+1)$ 中的两个系数都是1,它们全都不是2的倍数。因此 $x(x+1)$ 并不是绝对同余式。

这里要注意的地方是方程的解在一般情况下是一些个别的数,而同余式的解包含无穷多个数。如果其中一个数是同余式的解,那么与这个数同余的数就都是同余式的解,我们把属于同一个同余类的解都看成相同的解。由这一说明立刻就得出:

定理 3.9.1 设同余式方程的模是 m,那么同余式方程 $f(x)\equiv 0(\mathrm{mod}\ m)$ 至多有 m 个解。

虽然我们在形式上定义了同余式方程的元数的概念,但是我们通常只讨论一元的同余式方程,并且不考虑模为未知数的同余式方程。

关于同余式的同解性,有一些与方程类似的判定法则,但也有一些不同的地方。

上面中表8.中的法则对于方程和同余式方程虽然有所差别,但是毕竟还有相似之处。然而下面这一法则却是同余式方程所特有的了。

定理 3.9.2 设同余式方程的模是 $m>0$,同余式方程的两边和模 m 有大于1的最大公约数,即同余式方程可写成 $kg(x)\equiv 0(\mathrm{mod}\ km)$ 的形式,其中 $g(x)$ 的系数中至少有一个是与 m 互素的。

又设同余式方程 $g(x)\equiv 0(\mathrm{mod}\ m)$ 的解数是 s,那么同余式方程 $kg(x)\equiv 0(\mathrm{mod}\ km)$ 的解数就是 ks。

证明 设同余式方程 $g(x)\equiv 0(\mathrm{mod}\ m)$ 的一个解是 c,那么 $0\leqslant c<m$。且 $g(c)\equiv 0(\mathrm{mod}\ m)$。又设 $z_i=c+im$,$i=0,1,2,\cdots,k-1$,则显然 $z_i\equiv$

$c(\mathrm{mod}\ m)$，因此 $g(z_i)\equiv 0(\mathrm{mod}\ m)$。根据同余式的意义，必有整数 y 使得 $g(z_i)-my=0$，因此有 $kg(z_i)-kmy=0$，或者 $kg(z_i)\equiv 0(\mathrm{mod}\ km)$，这就说明 $z_i=c+im, i=0,1,2,\cdots,k-1$ 都是同余式方程 $kg(x)\equiv 0(\mathrm{mod}\ km)$ 的解，这就证明了定理。

根据上面的同解法则和定理就可以得出：

引理 3.9.1 任何同余式方程都可以化为下面的标准形：$f(x)\equiv 0(\mathrm{mod}\ m)$，使得 $f(x)\equiv 0(\mathrm{mod}\ m)$ 和原来的同余式方程同解，且

(1) $f(x)$ 的系数中没有 m 的倍数，且都小于 m；

(2) $f(x)$ 的次数小于 m；

如果 $f(x)$ 的系数和 m 的最大公约数为 $k>1$，那么可以把 k 约去使得

(3) $f(x)$ 的系数和 m 的最大公约数为 1。

这时原来的同余式方程的解数是 $f(x)\equiv 0(\mathrm{mod}\ m)$ 的解数的 k 倍，这 k 倍个解可以应用定理 3.9.2 从 $f(x)\equiv 0(\mathrm{mod}\ m)$ 的解得出。

下面我们就来介绍各种现在已知的同余式方程的结果。

首先讨论最简单的一次同余式方程，即

$$ax\equiv b(\mathrm{mod}\ m),(a,m)=1$$

根据第 5 节中关于一次不定方程的讨论，解上面的同余式方程就相当于求不定方程

$$ax-my=b$$

的整数解。于是根据第 5 节中关于一次不定方程的讨论的内容立刻就得到。

定理 3.9.3 当 $(a,m)=1$ 时，同余式方程 $ax\equiv b(\mathrm{mod}\ m)$ 有唯一解。

证明 解的存在性由第5节中关于一次不定方程的讨论立刻得出，现在证明唯一性。设 c_1,c_2 都是同余式方程 $ax\equiv b(\mathrm{mod}\ m)$ 的解，则 $ac_1\equiv b(\mathrm{mod}\ m)$，$ac_2\equiv b(\mathrm{mod}\ m)$，因此 $a(c_1-c_2)\equiv 0(\mathrm{mod}\ m)$，故 $m\mid a(c_1-c_2)$，但是由于 $(a,m)=1$，因此就得出 $m\mid(c_1-c_2)$ 或者 $c_1\equiv c_2(\mathrm{mod}\ m)$，根据我们对同余式方程解的定义就证明了解的唯一性。

对于一般的一次同余式方程，根据定理3.9.2和定理3.9.3以及第5节中关于一次不定方程的讨论就得出

定理 3.9.4 设 $k=(a,m)$，则同余式方程 $ax\equiv b(\mathrm{mod}\ m)$ 有解的充分必要条件为 $k\mid b$。当 $k\mid b$ 时，由定理3.9.3知同余式方程 $\frac{a}{k}x\equiv\frac{b}{k}\left(\mathrm{mod}\ \frac{m}{k}\right)$ 有唯一解 $x=c$，那么同余式方程 $ax\equiv b(\mathrm{mod}\ m)$ 的全部解即为 $c+\frac{m}{k}i, i=0,1,2,\cdots,k-1$。故同余式方程在有解时的解数为 (a,m)。

至于具体如何求出这个解来，我想如果你对前面的内容都很仔细地看了，并且都弄懂了的话应该是不成问题的。为了让你省事，再来回往前翻，我在这再

重复一下：

1. 试验的方法

因为同余式方程的解是有限的，所以原则上总是可以通过实验的方法求出解来的；

2. 欧拉定理法

设$(a,m)=1$，则由欧拉定理知 $a^{\varphi(m)}\equiv 1(\mathrm{mod}\ m)$，因此在同余式方程 $ax\equiv b(\mathrm{mod}\ m)$ 的两边同乘以 $a^{\varphi(m)-1}$ 即可得到 $x\equiv a^{\varphi(m)-1}b(\mathrm{mod}\ m)$。再求出 $a^{\varphi(m-1)}b$ 除以 m 的余数，就求出了同余式方程 $ax\equiv b(\mathrm{mod}\ m)$ 的唯一解。

不过我告诉你一句老实话，上述办法都只对模比较小（手上有一个计算器的话，大概对小于 100 的模还是可以忍受的吧）的情况可以用，如果模很大，那恐怕没有谁会有什么高招。那只有老老实实地用老办法即

3. 辗转相除法

设$(a,m)=1$，要解同余式 $ax\equiv b(\mathrm{mod}\ m)$。可以把它化为不定方程 $ax-my=b$，然后应用定理 3.5.1（也就属应用辗转相除法）就可求出方程 $ax-my=b$ 的一组特解，再把解中的 x 对模 m 求余数，就得到同余式方程 $ax\equiv b(\mathrm{mod}\ m)$ 的唯一解。

总结以上的讨论，可以得出解一般的一次同余式方程 $ax\equiv b(\mathrm{mod}\ m)$ 的步骤如下：

(1) 设 $k=(a,m)$，首先检查是否有 $k=1$，如果 $k=1$，那么同余式方程 $ax\equiv b(\mathrm{mod}\ m)$ 有唯一解，此唯一解可用上面提到的各种方法求出；

(2) 如果 $k>1$，则检查 $k\mid b$ 是否成立，如果 $k\nmid b$，则同余式方程 $ax\equiv b(\mathrm{mod}\ m)$ 无解，步骤停止；

(3) 如果 $k\mid b$，则说明 a,b,m 有公因数，因而可考虑同余式方程

$$\frac{a}{k}x\equiv\frac{b}{k}\left(\mathrm{mod}\ \frac{m}{k}\right),\left(\frac{a}{k},\frac{m}{k}\right)=1$$

这时方程已化成为标准形。

(4) 对以上的同余式方程用上面提到的各种方法求出一个唯一解；

(5) 应用定理 3.9.4 求出原来的同余式方程的 k 个解。

例 3.9.1 解同余式方程 $58x\equiv 87(\mathrm{mod}\ 47)$。

解 首先将其化为标准形 $11x\equiv 40(\mathrm{mod}\ 47)$，由于$(11,47)=1$，所以此方程有唯一解。由于模不太大，不妨用实验的方法去求。从 $x=1$ 开始试验起，以后每增加 1，余数就增加 11，因此可以得出下表，表中的数是用 x 代进去后再除以 47 的余数。

$$11,22,33,44,55\equiv 8,19,30,41,52\equiv 5,16,27,38,49\equiv 2,13,24,35,46\equiv -1,10,21,32,43\equiv -4,7,18,29,40$$

试验到此停止，由于40位于上表中的第25个位置上，因此我们就得出此同余式方程的解为

$$x \equiv 25 \pmod{47}$$

例 3.9.2 解同余式方程$78x \equiv 57 \pmod{93}$。

解 显然 78 和 93 都含有因子 3，因此我们有

$$(78,93) = 3(26,31) = 3$$

又 57 显然也是 3 的倍数：$57 = 3 \cdot 19$，因此从原来的同余式方程中约去 3 得到如下标准形

$$26x \equiv 19 \pmod{31}$$

这个模比上例还小，因此仍然可以用实验的方法得出：

$$26, 52 \equiv 21, 47 \equiv 16, 42 \equiv 11, 37 \equiv 6, 32 \equiv 1$$

试验至此停止，由于 32 位于第 6 个位置上，这就说明 $26 \cdot 6 \equiv 1$，由此得出

$$x \equiv 6 \cdot 19 \equiv 21$$

而原来的同余式的解就是 $21, 21 + 31 = 52$ 和 $21 + 2 \cdot 31 = 83$

例 3.9.3 解同余式方程 $589x \equiv 1\,026 \pmod{817}$。

解 借助于计算器首先算出$\sqrt{589} = 24.26\cdots$ 因此 589 的最小素因数只能是 2,3,5,7,11,13,17,19,23。显然 2,3,5 都不可能是 589 的因数，因此从 7 开始试除，试除到 19，发现 $589 = 19 \cdot 31$. 试除至此结束，然后用 19 去除 817 发现 $817 = 19 \cdot 43$，因此得出 $k = (589,817) = 19$。再用 k 去除 1 026 发现 $1\,026 = 19 \cdot 54$。因此同余式两边及模可以用 19 去约而得到如下标准形

$$31x \equiv 54 \pmod{43} \text{ 或 } 31x \equiv 11 \pmod{43}$$

对 31 和 43 实行辗转相除法如下

$$31 = 0 \cdot 43 + 31, 0 < 31 < 43, q_1 = 0$$

$$43 = 1 \cdot 31 + 12, 0 < 12 < 31, q_2 = 1$$

$$31 = 2 \cdot 12 + 7, 0 < 7 < 12, q_3 = 2$$

$$12 = 1 \cdot 7 + 5, 0 < 5 < 7, q_4 = 1$$

$$7 = 1 \cdot 5 + 2, 0 < 2 < 5, q_5 = 1$$

$$5 = 2 \cdot 2 + 1, 0 < 1 < 2, q_6 = 2$$

$$2 = 2 \cdot 1$$

$$p_0 = 1, p_1 = 0, p_2 = 1 \cdot 0 + 1 = 1, P_3 = = 2 \cdot 1 + 0 = 2$$

$$Q_0 = 0, Q_1 = 1, Q_2 = 1 \cdot 1 + 0 = 1, Q_3 = 2 \cdot 1 + 1 = 3$$

$$P_4 = 1 \cdot 2 + 1 = 3, P_5 = 1 \cdot 3 + 2 = 5, P_6 = 2 \cdot 5 + 3 = 13$$

$$Q_4 = 1 \cdot 3 + 1 = 4, Q_5 = 1 \cdot 4 + 3 = 7, Q_6 = 2 \cdot 7 + 4 = 18$$

计算至此结束，然后通过实验发现

$$31 \cdot 18 - 43 \cdot 13 = -1$$

因此 $$31 \cdot (-18) - 43 \cdot (-13) = 1$$

或者 $$31 \cdot (-18 \cdot 11) - 43 \cdot (-13 \cdot 11) = 11$$

即 $-18 \cdot 11 \equiv 17$ 是 $31x \equiv 11 \pmod{43}$ 的唯一解，而原同余式方程的解就是从17逐次加上43直到再加就超过817的所有数，也就是17,60,103,146,189,232,275,318,361,404,447,490,533,576,619,662,705,748,791这19个数。

所以现在的问题就是是不是能够把一个同余式方程化成模小一点的同余式方程去解了。如果同余式方程的模是一个素数而又很大，那么我告诉你，趁早不要去想什么邪门歪道，只有老老实实地该怎么解就怎么解，但是如果模是一个复合数，那么可以用下面的方法化简。

定理 3.9.5 设 $m_1, m_2, \cdots, m_k$ 两两互素，$m = m_1 m_2 \cdots m_k$，那么同余式方程

$$f(x) \equiv 0 \pmod m$$

与同余式方程组 $f(x) \equiv 0 \pmod{m_1}, f(x) \equiv 0 \pmod{m_2}, \cdots, f(x) \equiv 0 \pmod{m_k}$ 同解。

证明 设 $x = c, 0 \leqslant c < m$ 是同余式方程 $f(x) \equiv 0 \pmod m$ 的解，则 $f(c) \equiv 0 \pmod m$，那么由 $m = m_1 m_2 \cdots m_k$ 和同余式的性质（定理3.6.3）可知 $f(c) \equiv 0 \pmod{m_i}, i = 1,2,\cdots,k$。这就说明同余式方程 $f(x) \equiv 0 \pmod m$ 的解都是同余式方程组 $f(x) \equiv 0 \pmod{m_i}, i = 1,2,\cdots,k$ 的解。

反过来，如果 $x = c, 0 \leqslant c < m_i$ 是同余式方程组 $f(x) \equiv 0 \pmod{m_i}, i = 1,2,\cdots,k$ 的解，那么 $f(c) \equiv 0 \pmod{m_i}, i = 1,2,\cdots,k$ 由 $m_1, m_2, \cdots, m_k$ 两两互素和同余式的性质（定理3.6.4(9)）可知 $f(c) \equiv 0 \pmod m$，这就说明同余式方程组 $f(x) \equiv 0 \pmod{m_i}, i = 1,2,\cdots,k$ 的解都是同余式方程 $f(x) \equiv 0 \pmod m$ 的解。

根据这个定理，我们只要会解同余式方程组，就可以把解复合模同余式方程的问题化为解同余式方程组的问题了。然而我们首要要弄清楚什么是同余式方程组的不同的解。

设 $f_i(x) \equiv 0 \pmod{m_i}, i = 1,2,\cdots,k$ 是同余式方程组，$x = c$ 是这一方程组的一个解。这也就是说整数 c 同时满足 k 个同余式方程，即使得

$$f_i(x) \equiv 0 \pmod{m_i}, i = 1,2,\cdots,k$$

同时成立，那么根据同余式的性质（定理3.6.3）显然同余类 $c \pmod m$ 中的任何一个整数也都是同余式方程组 $f_i(x) \equiv 0 \pmod{m_i}, i = 1,2,\cdots,k$ 的一个解，这里 $m = [m_1 m_2 \cdots m_k]$ 是 $m_1, m_2, \cdots, m_k$ 的最小公倍数。这一事实可以记为 $x \equiv c \pmod m$ 是同余式方程组 $f_i(x) \equiv 0 \pmod{m_i}, i = 1,2,\cdots,k$ 的解。根据这一说明，只有当 c_1, c_2 都是同余式方程组 $f_i(x) \equiv 0 \pmod{m_i}, i = 1,2,\cdots,k$ 的

解并且对模 m 不同余时才把它们看成是同余式方程组 $f_i(x)\equiv 0(\bmod m_i), i=1,2,\cdots,k$ 的不同的解。我们把所有对模 m 两两不同余的解的个数称为是同余式方程组 $f_i(x)\equiv 0(\bmod m_i), i=1,2,\cdots,k$ 的解数。因此,我们只须在模 m 的余数中去求解同余式方程组 $f_i(x)\equiv 0(\bmod m_i), i=1,2,\cdots,k$,它的解数最多为 m 个。

下面我们就来研究如何解最简单的同余式方程组。最简单的同余式方程组的形式为

$$x\equiv b_i(\bmod m_i), i=1,2,\cdots,k$$

其中 $m_1,m_2,\cdots,m_k$ 是两两互素的正整数。

关于它的解数,我们有

定理 3.9.6 设 $m_1,m_2,\cdots,m_k$ 是两两互素的正整数,那么同余式方程组 $x\equiv b_i(\bmod m_i), i=1,2,\cdots,k$ 如果有解,则它的解是唯一的。

证明 设 c_1,c_2 都是同余式方程组 $x\equiv b_i(\bmod m_i), i=1,2,\cdots,k$ 的解,那么

$$c_1\equiv b_i(\bmod m_i), i=1,2,\cdots,k, c_2\equiv b_i(\bmod m_i), i=1,2,\cdots,k$$

因此

$$c_1\equiv c_2(\bmod m_i), i=1,2,\cdots,k$$

由于 $m_1,m_2,\cdots,m_k$ 两两互素,故由同余式的性质(定理 3.6.4(9))即得 $c_1\equiv c_2(\bmod m)$。

于是根据上面我们对同余式方程组解的说明,它们被看成是同一个解。这就证明了定理。

上面的定理只肯定了如果同余式方程组 $x\equiv b_i(\bmod m_i), i=1,2,\cdots,k$ 有解,则它的解必是唯一的。但是并没有说明它是否一定有解。我们下面就来证明这一方程组必定有解。我们所采用的方法可称为单因子构建法。这一方法的实质就是先设法让其他因素不起作用,而只先考虑一个因素的作用,再把所得的结果叠加起来就得到整体的结果,整个过程好像搭积木一样。为此,我们考虑 k 个方程组如下

$$(1)\ x\equiv 1(\bmod m_1), x\equiv 0(\bmod m_2),\cdots, x\equiv 0(\bmod m_k)$$

$$(2)\ x\equiv 0(\bmod m_1), x\equiv 1(\bmod m_2),\cdots, x\equiv 0(\bmod m_k)$$

$$\vdots$$

$$(k)\ x\equiv 0(\bmod m_1), x\equiv 0(\bmod m_2),\cdots, x\equiv 1(\bmod m_k)$$

于是显然如果第一个方程组的解是 $x\equiv c_1(\bmod m_i), i=1,2,\cdots,k$,第二个方程组的解是 $x\equiv c_2(\bmod m_i), i=1,2,\cdots,k,\cdots$,第 k 个方程组的解 $x\equiv c_k(\bmod m_i), i=1,2,\cdots,k$,那么同余式方程组 $x\equiv b_i(\bmod m_i), i=1,2,\cdots,k$ 的解就是 $x\equiv c_1b_1+c_2b_2+\cdots+c_kb_k$。这一事实可以称为线性同余式方程组的迭加原理。

现在我们就来研究每一个方程组是否有解。先看第一个方程组

$$x \equiv 1(\text{mod } m_1), x \equiv 0(\text{mod } m_2), \cdots, x \equiv 0(\text{mod } m_k)$$

由后面几个方程可以看出 x 必是 $m_2, \cdots, m_k$ 的倍数，因而必是 $M_1 = m_2 \cdots m_k = \frac{m}{m_1}$ 的倍数。也就是可设 $x = M_1 y$。由于 $m_2, \cdots, m_k$ 是两两互素的，因此必有 $(M_1, m_1) = 1$，故由定理 3.9.3 可知同余式方程 $M_1 y \equiv 1(\text{mod } m_1)$ 必有唯一解 $y \equiv M'_1(\text{mod } m_1)$，即 $x = M_1 y \equiv M_1 M'_1(\text{mod } m_1)$，由 M_1 的定义我们知当 $i \neq 1$ 时 $m_i \mid M_1$，因此 $x = M'_1 M_1 \equiv 0(\text{mod } m_i)$，$i = 2, 3, \cdots, k$。这就说明 $x = M'_1 M_1$ 就是方程组(1) 的解。

同理，对其他的每个方程，定义 $M_i = \frac{m}{m_i}$，$i = 2, 3, \cdots, k$，那么用同样的方式可以证明 $x = M'_2 M_2$ 是方程组(2) 的解，…，$x = M'_k M_k$ 是方程组(k) 的解。因此根据上面所说的迭加原理即得出 $x \equiv M'_1 M_1 b_1 + M'_2 M_2 b_2 + \cdots + M'_k M_k b_k$ 是同余式方程组 $x \equiv b_i(\text{mod } m_i)$，$i = 1, 2, \cdots, k$ 的解。再由定理 3.9.6 知，这个解是唯一的，因此方程组 $x \equiv b_i(\text{mod } m_i)$，$i = 1, 2, \cdots, k$ 的任意解比可表示成为上述形式。

孙子(3—4世纪)，中国数学家，生卒年代不可考，曾著《孙子算经》。

这样我们就得出如下以孙子命名的定理(国外一般称为中国剩余定理)。

定理 3.9.7(孙子定理或中国剩余定理) 设 $m_1, m_2, \cdots, m_k$ 是两两互素的正整数

$$m = m_1 m_2 \cdots m_k, M_i = \frac{m}{m_i}, i = 1, 2, \cdots, k$$

因此 $(M_i, m_i) = 1$，$i = 1, 2, \cdots, k$，而同余式方程 $M_i x \equiv 1(\text{mod } m_i)$ 必有唯一解。

$$x \equiv M'_i(\text{mod } m_i)$$

那么同余式方程组 $x \equiv b_i(\text{mod } m_i)$，$i = 1, 2, \cdots, k$ 的解可表示成

$$x \equiv M'_1 M_1 b_1 + M'_2 M_2 b_2 + \cdots + M'_k M_k b_k$$

上面这个定理之所以以孙子的名字命名，是因为它最早来源于我国古代的一部优秀数学著作《孙子算经》。

中国许多其他的数学文献如《夏侯阳算经》和《张邱建算经》都提到过它(这部著作的确切出版年月已无从考证)。其中载有“物不知其数”的一个问题如下：

“今有物不知其数，三三数之胜(念剩，与剩字是同一个字的不同写法)二，五五数之胜三，七七数之胜二，问物几何。”

把这个问题翻译成现代汉语就是“有一堆物品三个三个地数，最后剩下两个，五个五个地数，最后剩下三个，七个七个地数，最后剩下两个，问这堆物品共有多少。”



我国古代数学文献《张邱建算经》
中关于孙子问题的记载

这类的问题在我国古代历史上还有许多其他的名称，如“鬼谷算”，“秦王暗点兵”（有的文献中称为“韩信点兵”），还有“剪管术”，“隔墙算”，“神机妙算”，“大衍求一术”，等等。其解法在程大位所著的《算法统宗》(1583 年) 中概括为以下一首诗：

三人同行七十稀，
五树梅花廿一枝，
七子团圆月正半，
除百零五便得知。

这首诗的含义到底是什么即使我们到现在也看不出来，在古代数学知识很不普及，数学文献难以得到，全靠宗师口传心授的时代，更是显得神秘莫测。掌握这一套算法的人，背下来这首诗，就可以当场显灵，让一方阵士兵一二一二，一二三一二三这样的报几遍数即可马上得知人数，而其他人则看得一头雾水，对军师、丞相一类的神人佩服得五体投地。这还算是用在正地方上了，如果被心怀叵测的小人学了去，则可能把老实的百姓骗得一愣一愣的。现在我们就来破解一下这首诗的含义。

用我们刚刚讲过的孙子定理来解上面所说的物不知其数问题就有

$$m_1 = 3, m_2 = 5, m_3 = 7, b_1 = 2, b_2 = 3, b_3 = 2$$

$$m = 105, M_1 = 35, M_2 = 21, M_3 = 15$$

解同余式方程 $35y \equiv 1 \pmod 3$ 可得 $M'_1 = 2$，解同余式方程 $21y \equiv 1 \pmod 5$ 可得 $M'_2 = 1$，解同余式方程 $15y \equiv 1 \pmod 7$ 可得 $M'_3 = 1$，于是根据

孙子定理，物不知其数，问题的解就是

$$x\equiv M'_1M_1b_1+M'_2M_2b_2+M'_3M_3b_3=35\cdot2\cdot2+21\cdot1\cdot3+15\cdot1\cdot2=$$
$$70\cdot2+21\cdot3+15\cdot2=233\equiv23(\mathrm{mod}\ 105)$$

现在你可以看出这首诗的奥秘了吧，原来诗里的三、五、七就是问题中出现的三个模。七十、廿一和月正半（即十五）分别就是孙子定理的公式中对应于模3,5,7也就是 b_1,b_2,b_3 之前的系数，而105就是那个大模 m。所以这首诗背后的实质便是孙子定理，任何一个人只要背下来这首诗，再碰到物不知其数类的问题，只要在那几个余数之前乘上这三个系数，再把它们加起来，如果得数大于105，则从得数中连续减去105最后所得的小于105的数就是答案了（你自己可以证明，最多减去两个105得数便会小于105了）。至于为什么要减去105，原因在于前面我们已经证明过，对那几个小模同时同余的数一定也是对大模同余的，所以减去105的结果一是可以得出一个最小解，二是只有用那个大模做标准，才能区分出全部情况，即在取3,5,7做模时，最多可能有105种情况，也才能看出两个解是否同一（在对大模同余的意义下）。

哈哈，秘密一旦揭穿也不过尔尔，你现在已掌握了这套算法了，不但如此，你自己可以把那几个模换成其他的模，去得出另外的公式并预先记住那几个系数而去跟你的朋友表演一番，你的朋友之中即使有人会解同余式，要想立刻就把那几个系数算出来恐怕也不轻松，何况现在对数学真感兴趣，苦心钻研的人并不多，所以你几乎有百分之九十的胜算。而你如果到了古代，肯定要被人看成高人了，不过我在第一章中就已说过，你也可能被看成巫师一类的人物，所以想事情不要光想好的方面。

其实，如果单纯是为了解决物不知其数问题，根本不需要这么费劲，也不需要学什么同余式。因为从3除余2,7除余2立刻可以得出21除余2，具有这种性质的最小的正整数就是23，它刚好是5除余3的数，所以如果你想到这些的话，不到一分钟，甚至半分钟就可以得出答案。但是这种解法如果换了其他的余数就不见得这么顺利了。不信你可以算一下被3可以除尽，5除余2,7除余4的问题。所以程大位书里的这首诗表明它是有一个公式的，这正是孙子定理的价值之一，上面那个问题用孙子定理同样可很快得出答案，而且由于有一个余数是零，因此只要算两个系数即可。可惜中国古代的数学家对得出的结果往往只是用具体的数字例子说明，而不写出一个普适的公式，不过从国外把孙子定理称为中国剩余定理来看，他们还是承认中国人在古代就知道这一公式的。

这里我们再顺便说一下与这个问题有关的几个人。

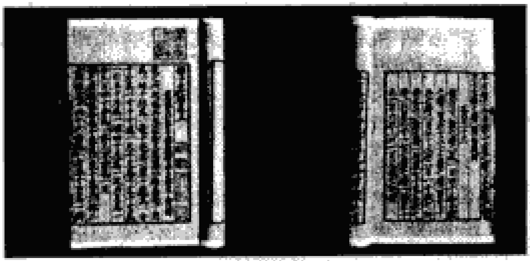
中国古代被称为孙子的有两个人，一个是春秋末期时代的军事家，叫孙武。举世闻名的《孙子兵法》就是他著的。

还有一个军事家叫孙膑，是战国时代的人，他是孙武的后代，大致与商鞅、

孟子是同时代的人，著有《孙膑兵法》，他曾与庞涓同学兵法，后来庞涓到魏国做了将军，但时时担心才能不如孙膑，将来可能败于他之手，因此假以同学情谊，花言巧语把孙膑骗到魏国，然后幕搞阴谋诡计，向魏王秘密汇报假情况而借魏王之手将孙处以膑刑(去掉膝盖骨)，故被称之为孙膑，后来孙膑在被禁闭期间装疯使他放松了警惕，被齐国使者秘密接走，被齐威王任为军师。他设计先后大败魏军于桂陵和马陵，最后终于在马陵之战中将庞涓杀死，据说，庞涓进入包围圈后见到一个大树，其一侧树皮被刮光，上写庞涓死于此树之下，庞涓大惊，急令撤退，但已来不及，被乱箭射死，可见其算度之精。

还有一个叫鬼谷子的人，相传是战国时楚国人。姓名传说不一，隐居于鬼谷，因此自号鬼谷子。长于养性持身和纵横捭阖之术。

这三个人从才能上和时代上讲，都可能是《孙子算经》的作者，但是至今无法确认其作者和出版年代。然而无论如何"物不知其数"问题是世界上公认的中国古代的重要工作。是我们炎黄子孙值得自豪的数学成果之一。



《孙子算经》(宋刻本)

有了孙子定理，我们就可证明下面这个把大模化成小模后原方程和化完后所得的小模方程的解数关系的公式了。

定理 3.9.8 设 $m_1,m_2,\cdots,m_k$ 两两互素，$m=m_1m_2\cdots m_k$。如果用 T_i 表示同余式方程 $f(x)\equiv 0(\text{mod }m_i)$ 的解数，$i=1,2,\cdots,k$。用 T 表示同余式方程 $f(x)\equiv 0(\text{mod }m)$ 的解数，则 $T=T_1T_2\cdots T_k$。

证明 设 $f(x)\equiv 0(\text{mod }m_i)$ 的 T_i 个解为

$$x\equiv c_{1t_1}(\text{mod }m_1),x\equiv c_{1t_2}(\text{mod }m_2),\cdots,x\equiv c_{1t_k}(\text{mod }m_k)$$

其中 $t_i=1,2,\cdots,T_i,i=1,2,\cdots,k$。

那么把这些解组合起来就得到一些同余式方程组，其中第一个方程有 T_1 种可能，即第一个方程可能是 $x\equiv c_{11}(\text{mod }m_1),x\equiv c_{12}(\text{mod }m_1),\cdots$，或者 $x\equiv c_{1k}(\text{mod }m_1)$。同理第二个方程有 T_2 种可能，$\cdots$，第 k 个方程有 T_k 种可能。所以组合起来共有 $T=T_1T_2\cdots T_k$ 种可能。其中每一种可能的方程组根据孙子定理都有一个唯一解 $x\equiv c_{ij}$，而且前面我们已经证明，这些解都是同余于模 $m=m_1m_2\cdots m_k$ 的，所以它们都是同余式方程 $f(x)\equiv 0(\text{mod }m)$ 的解。下面我们来证

明他们对模 $m = m_1m_2\cdots m_k$ 是两两不同余的。设

(1) $x \equiv b_1 (\text{mod } m_1), x \equiv b_2 (\text{mod } m_2), \cdots, x \equiv b_k (\text{mod } m_k)$，以及

(2) $x \equiv c_1 (\text{mod } m_1), x \equiv c_2 (\text{mod } m_2), \cdots, x \equiv c_k (\text{mod } m_k)$。

是这些组合出来的方程组中的两个不同的方程组，那么必存在一个指标 h 使得 $b_h \neq c_h$。设方程组(1)的解是 $x = u$，方程组(2)的解是 $x = v$，那么由孙子定理知

$$u = M_1M'_1b_1 + M_2M'_2b_2 + \cdots + M_kM'_kb_k$$

$$v = M_1M'_1c_1 + M_2M'_2c_2 + \cdots + M_kM'_kc_k$$

如果 $u \equiv v (\text{mod } m)$，那么由于 $m = m_1m_2\cdots m_k$，所以必有 $u \equiv v (\text{mod } m_h)$。注意在孙子定理中我们已证明当 $i \neq h$ 时 $M_i \equiv 0 (\text{mod } m_h)$，而 $(M_hM'_h, m_h)$，因此就得出

$$M_hM'_hb_h \equiv M_hM'_hc_h (\text{mod } m_h)$$

故 $b_h \equiv c_h (\text{mod } m_h)$，再由 $0 \leqslant b_h < m_h, 0 \leqslant c_h < m_h$ 即得出 $b_h = c_h$，这与 $b_h \neq c_h$ 的假设矛盾。所得的矛盾就说明上述方程组的解对模 $m = m_1m_2\cdots m_k$ 是两两不同余的。这就证明方程 $f(x) \equiv 0 (\text{mod } m)$ 恰有 $T = T_1T_2\cdots T_k$ 个解。

现在你可以更明白“物不知其数”问题的解法中那个 105 的来历了，在此问题中，关于模 3，可能有 3 种余数，关于模 5，可能有 5 种余数，关于模 7，可能有 7 种余数。所以根据上面的定理，共可能有 $105 = 3 \cdot 5 \cdot 7$ 种情况。

至此，我们已经基本上解决了一次同余式方程组的求解问题。其求解步骤是：

(1) 首先检查方程组中的模是否是两两互素的，如果是，就转入步骤(2) 如果不是，则利用定理 3.9.5 将原来的方程组化为一个更大的模为两两互素的方程组；

(2) 利用孙子定理解所得的方程组。

例 3.9.4 求一最小的正数，被 10，3，7 和 11 除各剩下 4，2，3 和 1。

解 根据题意可列出同余式方程组如下

$$x \equiv 2 (\text{mod } 3)$$

$$x \equiv 3 (\text{mod } 7)$$

$$x \equiv 4 (\text{mod } 10)$$

$$x \equiv 1 (\text{mod } 11)$$

因此看出 $b_1 = 2, b_2 = 3, b_3 = 4, b_4 = 1, m = 3 \cdot 7 \cdot 10 \cdot 11 = 2\,310$。

为应用孙子定理，首先求出

$$M_1 = 7 \cdot 10 \cdot 11 = 770 \equiv 2 (\text{mod } 3)$$

$$M_2 = 3 \cdot 10 \cdot 11 = 330 \equiv 1 (\text{mod } 7)$$

$$M_3 = 3 \cdot 7 \cdot 11 = 231 \equiv 1 \pmod{10}$$
$$M_4 = 3 \cdot 7 \cdot 10 = 210 \equiv 1 \pmod{11}$$

然后求出

$$M'_1 = 2, M'_2 = 1, M'_3 = 1, M_4 = 1$$

由孙子定理即得

$$x \equiv 770 \cdot 2 \cdot 2 + 330 \cdot 1 \cdot 3 + 231 \cdot 1 \cdot 4 + 210 \cdot 1 \cdot 1 = 5\,204$$

最后再从 5 204 中连续减去 2 310 = 3 · 7 · 10 · 11 即得 $x = 584$。

例 3.9.5 某校学生有百人左右,7 人一组余 6 人,9 人一组余 7 人,12 人一组余 1 人,问学生数。

解 根据题意可列出同余式方程组如下

$$x \equiv 6 \pmod 7$$
$$x \equiv 7 \pmod 9$$
$$x \equiv 1 \pmod{12}$$

由于上面方程组中的模不是两两互素的,因此无法应用孙子定理。故第一步是把模化成为两两互素的情况。由定理 3.9.5 上面的方程组等价于方程组

$$x \equiv 1 \pmod 3$$
$$x \equiv 1 \pmod 4$$
$$x \equiv 6 \pmod 7$$
$$x \equiv 7 \pmod 9$$

这个方程组的模仍然不是两两互素的,但是由于对模 9 同余的数必定对模 3 同余,因此你需要检查模为 3 和 9 的两个方程是否相容(如果不相容,那原来的题目就不可能有解,所以他既然出这个题目,如果不是故意想要诈你,一般都应该是相容的)。经检查,由于

$$7 \pmod 9 \equiv 7 \pmod 3 \equiv 1 \pmod 3$$

故上面的方程是相容的,这样就可把上面的方程组化为下面的模是两两互素的方程组了(注意,在变化的过程中,你必须始终保持原始的大模不变,否则,就将丢失一些解,因此,你不能把原来的方程组化为下面的方程组去解。

$$x \equiv 1 \pmod 3$$
$$x \equiv 1 \pmod 4$$
$$x \equiv 6 \pmod 7$$

虽然它的模也是两两互素的,但是由于大模减小了,因此这个方程组是不符合要求的)

$$x \equiv 1 \pmod 4$$
$$x \equiv 6 \pmod 7$$
$$x \equiv 7 \pmod 9$$

对此方程组应用孙子定理即可求出解答,答案是 97。

孙子定理"物不知其数"问题出现后,虽然从历史上来说,这是最早的用公

式给出这一类问题的解答的文献。但是实际上，它只适用于模为 3，5，7 的情况，而且给出的公式中有三个数，即孙子定理中的 M'_1, M'_2, M'_3 是怎么来的也没有交代。因此在中国后来还有一些数学家对此加以研究，其中最突出的是南宋数学家秦九韶和清代学者黄宗宪。

1247 年秦九韶在《数书九章》一书中，解决了这个问题(即 M'_1, M'_2, M'_3 的来历问题)，并称其为"乘率"。

秦九韶在总结前人成果的基础之上，提出"大衍总数术"，从数的理论的角度，总结了求解一次同余式组的一般方法。把解法推广到模不是两两互素的一般情形。

据说对"大衍求一术"用的熟练的人算起"物不知其数"类的问题比用现代的同余式理论还要快，而且他这个"大衍求一术"的基础就是解同余式，所以许多可以化成为同余式的问题，如一次不定方程问题也都可以用这种方法去解，用途非常广泛。所以我们底下简单地介绍一下这种方法。为了容易看懂，我们首先把古代的一些术语和现代的同余式理论中的术语加以对照如下：

秦九韶方法	同余式理论
求数使 8 除余 5，15 除余 8，25 除余 13	解同余式方程组 $x \equiv 5 \pmod 8$ $x \equiv 8 \pmod{15}$ $x \equiv 13 \pmod{25}$
化问数为定数	把原来模不是两两互素的同余式方程组化为模是两两互素的方程组
原来的模 8，15，25 称为问数 化完后的模 3，8，25 称为定数	$x \equiv 8 \pmod 3 \equiv 2 \pmod 3$ $x \equiv 5 \pmod 8$ $x \equiv 13 \pmod{25}$ $m_1 = 3, m_2 = 8, m_3 = 25$
求"衍母"	$m = 3 \cdot 8 \cdot 25 = 600$
求"衍数"	$M_1 = \frac{m}{m_1} = 200$ $M_2 = \frac{m}{m_2} = 75$ $M_3 = \frac{m}{m_3} = 24$
求"奇数"	就是求 M_1, M_2, M_3 除以 m_1, m_2, m_3 所得的余数 $g_1 \equiv M_1 \equiv 2 \pmod 3$ $g_2 \equiv M_2 \equiv 3 \pmod 8$ $g_3 \equiv M_3 \equiv 24 \pmod{25}$
求"乘数"	就是解同余式方程 $gx \equiv 1 \pmod m$

到了这,就是秦九韶方法中最关键的部分了,他给出了一套算法第一步是"置寄右上,定居右下,天元一于左上。"先立一图式如下:

$$\begin{matrix} 1 & g \\ & m \end{matrix}$$

这句话的意思就是,在左上写上一个数 $p_0 = 1$,把奇数(这个奇数不是现代的奇数偶数的奇数,而是前面秦九韶定义的术语)写在右上,定数写在右下。

然后"先以右上除右下,所得商数与左上一相生,入左下,然后乃以后行上下,以少除多,递互除之,所得商数,随即递累乘,归左行上下,须使右上末后奇一而止,乃验左上所得,以为乘率。"

这段话的意思就是先用右上的数去除右下的数,再用所得的商去乘左上的数,然后把得数写在左下。以后就看右边的上下行哪个数大。用较小的数去除较大的数,所得的商数,随即乘以左上或左下的数(具体谁乘以谁,按照哪个方向,看完下面的例子后就会明白),再把得数和左下或左上的数相加,直到右上的数变为1,那时左上的数就是乘数。

举例如下:解同余式方程 $7x \equiv 1 \pmod{17}$。

$$\begin{matrix} 1 & 7 \\ & 17 \end{matrix}$$

令 $P_0 = 1$

↓

$$\begin{matrix} 1 & 7 \\ 2 & 3 \end{matrix}$$

用上面图中右上的7去除右下的17,商2余3,即 $q_1 = 2, r_1 = 3$,再用 $q_1 = 2$ 去乘左上的 $P_0 = 1$ 得 $P_1 = 2$

↓

$$\begin{matrix} 5 & 1 \\ 2 & 3 \end{matrix}$$

用上面图中右下的3去除右上的7,商2余1,即 $q_2 = 2, r_2 = 1$,再用 $q_2 = 2$ 去乘左下的 $P_1 = 2$ 再加上左上的 $P_0 = 1$ 得 $P_2 = 5$

因为右上已为1,所以计算至此结束,最后的答案,也就是要求的乘数就是左上的5。验算一下果然有 $7 \cdot 5 = 35 \equiv 1 \pmod{17}$。

把上面秦九韶的一般算法用现代的符号写出来就是

$$\begin{aligned} & && P_0 = 1 \\ m &= gq_1 + r_1, && P_1 = q_1 \\ g &= r_1 q_2 + r_2, && P_2 = q_2 P_1 + P_0 \\ r_1 &= r_2 q_3 + r_3, && P_3 = q_3 P_2 + P_1 \\ &\vdots && \\ r_{n-2} &= r_{n-1} q_n + r_n, && P_n = q_n P_{n-1} + P_{n-2} \end{aligned}$$

$$r_n = 1$$

哈，这怎么看着这么眼熟啊，这不就是辗转相除法吗？对了，你说得一点不错，这正是我们前面讲过的辗转相除法。所以秦九韶不过是创造出了一种执行辗转相除法的格式。明白了这个实质，你就不一定拘泥于它的格式了，只要你觉得方便、顺手，你完全可以用你自己喜欢的格式来做，在闵嗣鹤和华罗庚的书中都有他们自己认为方便的格式。

不过根据我们前面讲辗转相除法时所得的公式（见定理 3.3.7），我们只能得出

$$Q_n m - P_n g = (-1)^{n-1} r_n = (-1)^{n-1}$$

或者
$$P_n g - Q_n m = (-1)^n$$

所以形式上按照上面的秦九韶算法的格式不一定能保证求出来的乘数一定是一个正数，或者说，用这一算法其实最后不一定得出的是同余式方程

$$gx \equiv 1 \pmod m$$

的解，得出的也可能是同余式方程

$$gx \equiv -1 \pmod m$$

的解。例如从 $g = 37, m = 107$ 出发，按照秦九韶算法的格式将得到

$$\begin{matrix} 1 & 37 & & 1 & 37 & & 3 & 4 & & 3 & 4 \\ 107 & & \rightarrow & 2 & 33 & \rightarrow & 2 & 33 & \rightarrow & 26 & 1 \end{matrix}$$

这个对着右下 1 的左下的 26 就是答案，但是可以验证它是同余式方程 $37x \equiv -1 \pmod{107}$ 的解。这个问题对我们根本是无所谓的，只要再化一步就出来了。但是在秦九韶那个时代，大概即使是数学家也觉得使用负数有点别扭（虽然根据文献他们也有这个概念），所以他还要搞一点小花样，以保证最后得出的答案一定是同余式方程 $gx \equiv 1 \pmod m$ 的解（见下文）。

秦九韶的结论，被国际数学界誉为“中国剩余定理”。其实，秦九韶的方法当时还有些不够严密的地方，表述也很晦涩。

正因为秦九韶这个算法还比较复杂，而且叙述的比较晦涩，所以后来真正弄懂它的人并不多，以至竟一度失传了，因而，秦九韶之后，在中国有不少数学家对他的方法进行了一系列的训诂、改进，尤其是清代学者张敦仁、骆腾风、时日醇、黄宗宪等在这方面做出了贡献。其中尤以黄宗宪改进的算法最为简单，据使用过这些方法的人比较体会，确以黄宗宪的方法最简明快捷。在西方直到欧拉、拉格朗日、高斯才对此问题进行了较为深刻的研究，高斯的方法与秦九韶的方法非常相同，不过那已是 19 世纪了。

我们通过一个具体的例子解释黄宗宪的方法，

设衍数是 45，定母是 8。首先在纸上画三条竖线，在三条竖线之间首先并排写上衍数和定母，衍数写在左边，定母写在右边。然后在竖线左边对齐衍数写上

一个 1，称为寄数，定母的右边没有寄数。

然后在衍数和定母之间用大数累次减去小数，直至余数小于减数，如此反复进行，直至余数为 1。

在每次的余数的左边或右边（看减法在左边一行进行还是在右边一行进行）都写上一个寄数，写寄数的法则如下：

（1）减数没有寄数的，余数的寄数与被减数相同；

（2）被减数没有寄数的，余数的寄数为累减次数；

（3）减数和被减数都有寄数的，余数的寄数就等于减数的寄数乘以累减次数再加上被减数的寄数。

这样最后对着余数为 1 的寄数就是所求的乘数。

首先累减 8 共 5 次	1	45 40	8 5		其次累减 5 共一次
累减 3 共 1 次	1	5 3	3 2	1	累减 2 共 1 次
	2	2 1	1	3	
累减 1 共 1 次	5	1			

最后得出乘率是 5。

把黄宗宪的算法用现代的数学符号写出来就是

$1 = P_0$ P_2	g $q_2 r_1$	r_1 $q_3 r_2$	P_3
…	… r_{2n-2} $q_{2n} r_{2n-1}$	… r_{2n-3} $q_{2n-1} r_{2n-2}$	…
P_{2n}	r_{2n}	r_{2n-1}	P_{2n-1}

其中

$$G = q_0 m + g, 0 \leqslant g < m$$

$$m = q_1 g + r_1, 0 \leqslant r_1 < g \qquad Q_1 m - P_1 g = r_1$$

$$g = q_2 r_1 + r_2, 0 \leqslant r_2 < r_1 \qquad P_2 g - Q_2 m = r_2$$

$$\vdots \qquad \vdots$$

$$r_{2n-3} = q_{2n-1} r_{2n-2} + r_{2n-1}, 0 \leqslant r_{2n-1} < r_{2n-2} \qquad Q_{2n-1} m - P_{2n-1} g = r_{2n-1}$$

$$r_{2n-2} = q_{2n} r_{2n-1} + r_{2n}, 0 \leqslant r_{2n} < r_{2n-1} \qquad P_{2n} g - Q_{2n} m = r_{2n}$$

因此我们立刻看出，这个黄宗宪算法和前面所介绍的秦九韶算法一样还是在计算 P_n，也就是他所说的寄数。不过这回他把寄数分成两边写，左边是下标

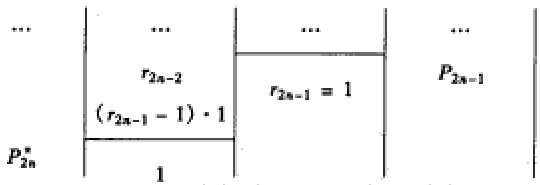
为偶数的寄数，右边为下标为奇数的寄数，所以显得更加简明。当左边的余数变为 1 时，根据我们上面的式子可知

$$P_{2n}g - Q_{2n}m = 1$$

所以乘数就是 P_{2n}。

当右边的余数变为 1 时，则有 $Q_{2n-1}m - P_{2n-1}g = 1$，或 $P_{2n-1}g \equiv -1(\mathrm{mod}\ m)$，这时按照现代的算法，我们可取 $-P_{2n-1}$ 或者 $-P_{2n-1} + km$ 作为乘数，因此可以结束计算。但是这就要用负数作为中介来计算，古代的数学家虽然已有负数的概念，但是似乎并没有像今天这样大规模和常规的使用习惯，所以当出现这种情况时，下面的计算就和现在的辗转相除法有一点小差别了(在没有出现数值为 1 的余数之前，所谓的累减次数和辗转相除法中的商数没有区别)。如果 $r_{2n-1} = 1$，那么在辗转相除法中的下一步就是 $r_{2n-2} = r_{2n-2} \cdot 1$，计算就此结束，然而这样就要得出 $P_{2n-1}g \equiv -1(\mathrm{mod}\ m)$。为了避免出现这种情况，黄宗宪算法的下一步却是

$$r_{2n-2} = (r_{2n-2} - 1) \cdot 1 + 1 \text{(如下图)}$$



这样数值为 1 的余数就出现在右边了，而相应的乘数为

$$P_{2n}^* = (r_{2n-2} - 1)P_{2n-1} + P_{2n-2}$$

但是为什么这个 P_{2n}^* 可以作为乘数呢，下面我们就来证明 P_{2n}^* 确实可以作为乘数。事实上，由于 $P_{2n-1}g - Q_{2n-1}m = -1$，所以

$$\begin{aligned}
P_{2n}^*G - 1 \equiv P_{2n}^*g - 1(\mathrm{mod}\ m) \equiv (P_{2n-1}(r_{2n-2} - 1) + P_{2n-2})g - 1(\mathrm{mod}\ m) &\equiv \\
(P_{2n-1}(r_{2n-2} - 1) + P_{2n-2})g + P_{2n-1}g - Q_{2n-1}m(\mathrm{mod}\ m) &\equiv \\
(P_{2n-1}(r_{2n-2} - 1) + P_{2n-2})g + P_{2n-1}g(\mathrm{mod}\ m) &\equiv \\
(P_{2n-1}(r_{2n-2} - 1) + P_{2n-2} + P_{2n-1})g(\mathrm{mod}\ m) &\equiv \\
(P_{2n-1}(r_{2n-2}g - 1) + P_{2n-2} + P_{2n-1})g(\mathrm{mod}\ m) &\equiv \\
(P_{2n-1}g - 1)P_{2n-2}g(\mathrm{mod}\ m) &\equiv \\
(Q_{2n-1}m)P_{2n-2}g(\mathrm{mod}\ m) &\equiv \\
0
\end{aligned}$$

这就证明了黄宗宪算法的合理性。看到这，我们不得不佩服我们的老祖先的智慧，因为按照黄宗宪的法则，得出这一步可以说是极为自然的，然而用现代的符号和理论，这一结论却不是一眼就能看出的。

在黄宗宪的《求一术通解》中还有利用反乘数来解"物不知其数"问题的算法，所谓反乘数，就是求同余式方程 $gx\equiv-1(\bmod m)$ 的解。这个按照我们上面的介绍如何求也是一目了然的了。就是在右边的余数变为1时，对着1的寄数就是反乘数。如果左边的余数先变成为1，那么可以用刚才右边的余数先变为1时最后一步的算法一样去处理。

上面介绍了我们中华民族在解一次同余式方程方面所取得的成就，在世界范围内，西方、印度和日本的数学家在不同的时期也都有人在不同程度上在这一问题上互相独立地取得了成果。为了比较这些成果的先后和水平，李倍始(U. Libbrecht)在其专著《13世纪的中国数学》中，从国际范围内数学发展的历史角度对各国数学的成果作了比较。我们认为，他的这一研究还是比较客观的。现介绍如下：

李倍始对一次同余式的成果提出了10个比较的标准：

(1) 提出问题，附特解，未叙述解法；

(2) 零散设题，算法限于一些特殊数据；

(3) 限于一套数据的某种算法；

(4) 限于特例的证明；

(5) 两两互素模的一般算法，未解；

(6) 两两互素模的一般算法，有解；

(7) 模不一定两两互素的一般算法，未证明；

(8) 模不一定两两互素的一般算法，并给出有解的条件；

(9) 给出两两互素模的一般算法的证明；

(10) 给出模不一定两两互素的一般算法的证明。

按照这10个标准，列表如下：

数学家或事件	年代	标准	1	2	3	4	5	6	7	8	9	10
《孙子算经》	约400?		√	√								
斐波那契 Leonardo Fibonacci	1202		√	√	√							
秦九韶	1247		√	√	√		√	√	√	√		
杨辉	1275		√	√	√							
严恭	1372		√									
阿古洛斯 I. Arguros	约1350		√	√								
慕尼黑手稿	约1450		√	√	√	√	?					
玉山若干 Rogiomontanus	约1460		√	?								
哥廷根手稿	约1550		√	√	√	√	√	√	√			

续表

程大位	1592	√	√								
休顿 V. Schooten	1657	√	√	√		√					
贝维立基 Beveridge	1669	√	√	√	√	√				√	
欧拉 L. Euler	1743	√	√	√	√	√	√			√	
高斯 F. C. Gauss	1801	√	√	√	√	√	√			√	
斯提尔吉斯 Stieljes	1890	√	√	√	√	√	√	√	√	√	√

对上述数学家按照这10个标准排出的工作质量前3名是:斯提尔吉斯;欧拉,高斯;秦九韶。以后的顺次排名是贝维立基,哥廷根手稿,休顿,慕尼黑手稿,斐波那契,杨辉,《孙子算经》,阿古洛斯,程大位,严恭,玉山若干。

这里秦九韶虽然排在第3名,然而按照时间顺序看,秦九韶达到水平(6),(7)的时间要比西方早300多年,达到水平(8)的时间比西方早了400多年,由此可见,秦九韶的"大衍求一术"在数学史上占有不可动摇的领先地位。

由素因子分解定理知任一个模 m 都可以写成 $m = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$ 的形式,再由定理3.9.5知要解同余式方程 $f(x) \equiv 0 \pmod m$ 可以归结为解同余式方程组 $f(x) \equiv 0 \pmod{p_i^{\alpha_i}}$, $i = 1,2,\cdots,k$。因此下面就来讨论同余式方程 $f(x) \equiv 0 \pmod{p^\alpha}$,$\alpha$ 是素数的解法。由同余式的性质知 $f(x) \equiv 0 \pmod{p^\alpha}$ 蕴含 $f(x) \equiv \pmod{p^{\alpha-1}}$,即 $f(x) \equiv 0 \pmod{p^{\alpha-1}}$ 是 $f(x) \equiv 0 \pmod{p^\alpha}$ 的必要条件。因此要求前者的解,可从后者的解出发。

定理 3.9.9 设 $\alpha \geqslant 2$, c 是同余式方程 $f(x) \equiv 0 \pmod{p^{\alpha-1}}$ 的解。那么

(1) 当 $p \nmid f'(c)$ 时,同余式方程组 $\begin{cases} f(x) \equiv 0 \pmod{p^\alpha} \\ x \equiv c \pmod{p^{\alpha-1}} \end{cases}$ 的解数为1;

(2) 当 $p \mid f'(c)$, $p^\alpha \nmid f(c)$ 时,同余式方程组 $\begin{cases} f(x) \equiv 0 \pmod{p^\alpha} \\ x \equiv c \pmod{p^{\alpha-1}} \end{cases}$ 无解;

(3) 当 $p \mid f'(c)$, $p^\alpha \mid f(c)$ 时,同余式方程组 $\begin{cases} f(x) \equiv 0 \pmod{p^\alpha} \\ x \equiv c \pmod{p^{\alpha-1}} \end{cases}$ 的解数为 p,即 $x \equiv 0,1,2,\cdots,p-1 \pmod p$ 都是这个方程组的解。

证明 由 $x \equiv c \pmod{p^{\alpha-1}}$ 得出 $x = c + p^{\alpha-1}y$,把此式代入同余式方程 $f(x) \equiv 0 \pmod{p_\alpha}$ 并把 $f(x)$ 在 $x = c$ 处展开即得

$$f(c) + f'(c)p^{\alpha-1}y \equiv 0 \pmod{p^\alpha}$$

故

$$f(c) + f'(c)p^{\alpha-1}y = Mp^\alpha$$

由于 c 是 $f(x) \equiv 0 \pmod{p^{\alpha-1}}$ 的解,因此 $p^{\alpha-1} \mid f(c)$,因此从上式推出

$$f'(c)y = -\frac{f(c)}{p^{a-1}} + Mp$$

或者
$$f'(c)y \equiv -\frac{f(c)}{p^{a-1}} \pmod p$$

从上面的式子就得出

(1) 如果 $p \nmid f'(c)$，那么 $(p, f'(c)) = 1$，因此一次同余式方程 $f'(c)y \equiv -\frac{f(c)}{p^{a-1}} \pmod p$ 有唯一解 $y \equiv b \pmod p$，由这个解就得出同余式方程组 $\begin{cases} f(x) \equiv 0 \pmod{p^a} \\ x \equiv c \pmod{p^{a-1}} \end{cases}$ 的唯一解 $x \equiv c + p^{a-1}b \pmod p$。

(2) 如果 $p \mid f'(c)$，$p^a \nmid f(c)$，那么 $f(c) \not\equiv 0 \pmod{p^a}$，那当然同余式方程组 $\begin{cases} f(x) \equiv 0 \pmod{p^a} \\ x \equiv c \pmod{p^{a-1}} \end{cases}$ 不可能有解了。

(3) 如果 $p \mid f'(c)$，$p^a \mid f(c)$，那么由直接验证即可知 $x \equiv 0, 1, 2, \cdots, p-1 \pmod p$ 都是方程 $f'(c)y \equiv -\frac{f(c)}{p^{a-1}} \pmod p$ 的解（实际上，这一方程现在已成为 $0 \cdot y \equiv 0 \pmod p$，当然任何一个数都是它的解）。而且不可能有其他解（因为此方程的模是 p，故最多有 p 个解）。因此这时方程组 $\begin{cases} f(x) \equiv 0 \pmod{p^a} \\ x \equiv c \pmod{p^{a-1}} \end{cases}$ 的解数就是 p。

由这个定理，我们就可从同余式方程 $f(x) \equiv 0 \pmod p$ 出发，逐步得到同余式方程 $f(x) \equiv 0 \pmod{p^a}$ 的解。

定理 3.9.10

(1) 设 c 是同余式方程 $f(x) \equiv 0 \pmod p$ 的解，且 $p \nmid f'(c)$，那么对任意 $a \geqslant 2$，同余式方程组 $\begin{cases} f(x) \equiv 0 \pmod{p^a} \\ x \equiv c \pmod{p^{a-1}} \end{cases}$ 的解数都为 1；

(2) 设同余式方程 $f(x) \equiv 0 \pmod p$ 和同余式方程 $f'(x) \equiv 0 \pmod p$ 没有公共解，那么对任意 $a \geqslant 1$，同余式方程 $f(x) \equiv 0 \pmod{p^a}$ 的解数都相同。

证明 (1) 设 c 是同余式方程 $f(x) \equiv 0 \pmod p$ 的解，由于 $p \nmid f'(c)$，因此一次同余式方程 $f'(c)y \equiv -\frac{f(c)}{p} \pmod p$ 有唯一解 $y \equiv b_1 \pmod p$，由这个解就得出同余式方程 $f(x) \equiv 0 \pmod{p^2}$ 的唯一解 $c_1 \equiv c + pb_1 \pmod p$。

由 $c_1 \equiv c + pb_1 \pmod p$ 是同余式方程 $f(x) \equiv 0 \pmod{p^2}$ 的解得出

$$f'(c_1) = f(c) + Mp$$

因此由 $p \nmid f'(c)$ 得出 $p \nmid f'(c_1)$，与前面一样因此一次同余式方程 $f'(c_1)y \equiv -\frac{f(c_1)}{p} \pmod{p^2}$ 有唯一解 $y \equiv b_2 \pmod{p^2}$，由这个解就得出同余式方程

$f(x)\equiv 0(\bmod p^3)$ 的唯一解 $c_2\equiv c_1+p^2b_2(\bmod p^2)$。…

依次类推，我们就得到对任意 $\alpha\geqslant 2$ 同余式方程组 $\begin{cases}f(x)\equiv 0(\bmod p^{\alpha})\\ x\equiv c(\bmod p^{\alpha-1})\end{cases}$ 的解数都为 1。

（2）由同余式方程 $f(x)\equiv 0(\bmod p)$ 和同余式方程 $f'(x)\equiv 0(\bmod p)$ 没有公共解立刻推出若 $x=c$ 是同余式方程 $f(x)\equiv 0(\bmod p)$ 的解，那么 $p\nmid f'(c)$（否则 $f(x)\equiv 0(\bmod p)$ 和 $f'(x)\equiv 0(\bmod p)$ 将有公共解 $x=c$）。因此由方程 $f(x)\equiv 0(\bmod p)$ 的每一个解就逐步得出方程 $f(x)\equiv 0(\bmod p)$，$\alpha\geqslant 1$ 的一个解，这些解就是 $f(x)\equiv 0(\bmod p^{\alpha})$ 的全部解，如果 $f(x)\equiv 0(\bmod p^{\alpha})$ 还有一个不是由方程 $f(x)\equiv 0(\bmod p)$ 的上述解得出的解，那么由于 $f(x)\equiv 0(\bmod p^{\alpha})$ 的解必为方程 $f(x)\equiv 0(\bmod p)$ 的解，因此我们就得到方程 $f(x)\equiv 0(\bmod p)$ 又有一个新解，而这是不可能的（因为我们在前面已经考虑了方程 $f(x)\equiv 0(\bmod p)$ 的全部解）。这就得出对任意 $\alpha\geqslant 1$，方程 $f(x)\equiv 0(\bmod p^{\alpha})$ 的解数与方程 $f(x)\equiv 0(\bmod p)$ 的解数相同。

例 3.9.6 解同余式方程 $x^3+5x^2+9\equiv 0(\bmod 3^4)$。

解 首先解同余式方程 $x^3+5x^2+9\equiv 0(\bmod 3)$，由于它的模是 3，所以通过简单实验就可得知它有两个解 $x\equiv 0$ 和 $x\equiv 1$。

$$f(x)=x^3+5x^2+9,f'(x)=3x^2+10x$$

$$f(0)=9,f(1)=15,f'(0)=0,f'(1)=13$$

又 $p=3$，所以 $p\mid f'(0),p^2\mid f(0),p\nmid f'(1)$ 所以根据定理 3.9.9 可知，$x=0,1,2$ 或者 $x=-1,0,1$ 全都是同余式方程 $f'(0)y\equiv-\dfrac{f(0)}{p}(\bmod p)$ 的解。而同余式方程 $f'(1)y\equiv-\dfrac{f(1)}{p}(\bmod p)$ 或者方程 $13y\equiv -5(\bmod 3)$ 有唯一解 $y=1$。

由此得出同余式方程 $x^3+5x^2+9\equiv 0(\bmod 3^2)$ 共有 4 个解，它们是

$$x=0+py=-3,0,3,x=1+py=4$$

再计算得出

$$f(-3)=27,f(0)=9,f(3)=81,f(4)=153$$

$$f'(-3)=-3,f'(0)=0,f'(3)=57,f'(4)=88$$

因此我们有 $p\mid f'(0),p\mid f'(-3),p\mid f'(3),p\nmid f'(4)$，再进一步检查得出 $p^3\nmid f(0),p^3\mid f(-3),p^3\mid f(3)$，所以 0 不是方程 $x^3+5x^2+9\equiv 0(\bmod 3^3)$ 的解。而 $y\equiv 0,1,2$ 都是方程

$$f'(-3)y\equiv-\frac{f(-3)}{p^2}(\bmod p)$$

和方程

$$f'(3)y\equiv-\frac{f(3)}{p^2}(\bmod p)$$

的解。方程

$$f'(4)y \equiv -\frac{f(4)}{p^2}(\bmod p)$$

或者

$$88y \equiv -17(\bmod 3)$$

有唯一解 $y=1$。由此得出 $x^3+5x^2+9\equiv 0(\bmod 3^3)$, $x\equiv 0(\bmod 3^2)$ 共有 7 个解，它们是

$$x=-3+p^2y=-2+9y=-3,6,15$$
$$x=3+p^2y=3+9y=3,12,21$$
$$x=4+p^2y=4+9y=13$$
$$f(-3)=27, f(3)=81, f(6)=405, f(12)=2\ 457$$
$$f(13)=3\ 051, f(15)=4\ 509, f(21)=11\ 475$$
$$f'(-3)=-3, f'(3)=57, f'(6)=168, f'(12)=552$$
$$f'(13)=637, f'(15)=825, f'(21)=1\ 533$$

因此

$$p \mid f'(-3), p^4 \nmid f(-3)$$
$$p \mid f(3), p^4 \mid f(3)$$
$$p \mid f'(6), p^4 \mid f(6)$$
$$p \mid f'(12), p^4 \nmid f(12)$$
$$p \mid f'(13)$$
$$p \mid f'(15), p^4 \nmid f(15)$$
$$p \mid f'(21), p^4 \mid f(21)$$

故 $y\equiv 0,1,2$ 都是方程

$$f'(3)y \equiv -\frac{f(3)}{p^3}(\bmod p)$$

和方程

$$f'(6)y \equiv -\frac{f(6)}{p^3}(\bmod p)$$

的解。方程

$$f'(13)y \equiv -\frac{f(13)}{p^3}(\bmod p)$$

或者

$$637y \equiv -113(\bmod 3)$$

有唯一解 $y=1$。由此得出 $x^3+5x^2+9\equiv 0(\bmod 3^4)$, $x\equiv 0(\bmod 3^3)$ 共有 7 个解，它们是

$$x=3+p^3y=3+27y=3,30,57$$
$$x=6+p^3y=6+27y=6,33,60$$
$$x=13+p^3y=13+27y=40$$

例 3.9.7 解同余式方程 $x^3+5x^2+9\equiv 0(\bmod 7\cdot 3^4)$。

解　由定理 3.9.5 知，这就是要解方程组

$$\begin{cases} x^3+5x^2+9\equiv 0 \pmod 7 \\ x^3+5x^2+9\equiv 0 \pmod{3^4} \end{cases}$$

由直接计算知第一个同余式方程的解为 $x\equiv 5 \pmod 7$，由例 3.9.6 知第二个同余式方程的解为 $x=3,6,30,33,40,57,60 \pmod{3^4}$，因而上述方程组最后化为 7 个一次同余式方程组（每个方程组含两个方程），由孙子定理即可得到解答，最后的答案是

$$x\equiv 33,40,138,222,327,411,516 \pmod{7\cdot 3^4}$$

现在来考虑在同余式中，多项式的析因子问题。

设 p 是一个素数，一个在模 p 下实质上是 n 次的多项式一定可以写成为

$$a_0x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n\equiv 0 \pmod p$$

的形式，其中 $(a_0,p)=1$，否则在模 p 下，n 次项将同余于 0，而因此这个多项式将不是 n 次的。因而，必存在一个整数 α 使得 $\alpha a_0\equiv 1 \pmod p$。用 α 去乘上述同余式即可将其化为

$$f(x)=x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n\equiv 0 \pmod p$$

之形，因此对于素数模来说，以后不妨总认为同余于此模的多项式的最高次数为 1。

现在设 $f(x)\equiv 0 \pmod p$ 有一个解 $x\equiv x_1 \pmod p$，那么根据多项式的带余数除法可以得到 $f(x)=(x-x_1)q_1(x)+f(x_1)$，但因为 $f(x_1)\equiv 0 \pmod p$，因此可把上式写为

$$f(x)\equiv (x-x_1)q_1(x) \pmod p$$

如果 $q_1(x)\equiv 0 \pmod p$ 又有解 $x\equiv x_2 \pmod p$，那么同理又可以把上面的式写为

$$f(x)\equiv (x-x_1)(x-x_2)q_2(x) \pmod p$$

如此继续下去，最后我们一定可把上式写为

$$f(x)\equiv (x-x_1)(x-x_2)\cdots(x-x_k)g(x) \pmod p$$

其中 $g(x)$ 是 $n-k\geqslant 1$ 次的整系数多项式，$x_1,x_2,\cdots,x_k$ 之中可能有相重的。且 $g(x)\equiv 0 \pmod p$ 没有解（这里不像在多项式理论当中那样，有一个代数基本定理保证在复数域中，任意多项式至少有一个根，例如由于 $0^2=0,(\pm 1)^2=1$，因此 $x^2\equiv 2 \pmod m$ 对任何 $m\geqslant 3$ 都没有解）。

反之，如果可把多项式 $f(x)$ 写成为

$$f(x)\equiv (x-x_1)(x-x_2)\cdots(x-x_k)g(x) \pmod p$$

的形式，其中 $g(x)$ 是 $n-k\geqslant 1$ 次的整系数多项式，$x_1,x_2,\cdots,x_k$ 之中可能有相重的，且 $g(x)\equiv 0 \pmod p$ 没有解，那么 $f(x)\equiv 0 \pmod p$ 的所有解就只能是

$x_1, x_2, \cdots, x_k$ 这 k 个解。假设不然，$f(x) \equiv 0 (\bmod p)$ 还有一个解 $x = \xi, \xi \not\equiv x_1, x_2, \cdots, x_k (\bmod p)$，那么把 $x = \xi$ 代入到 $f(x)$ 的表达式中去后就得到

$$(\xi - x_1)(\xi - x_2)\cdots(\xi - x_k)g(\xi) \equiv 0 (\bmod p)$$

但是因为 $g(x) \equiv 0 (\bmod p)$ 没有解，p 是素数，所以根据同余式的性质就得到必有某一个 x_i 使得 $\xi - x_i \equiv 0 (\bmod p)$，$\xi \equiv x_i (\bmod p)$，而这与我们的假设矛盾，所得的矛盾便证明了所要的结论。由此就得出下述定理：

定理 3.9.11 设在素数模 p 下，多项式 $f(x)$ 的所有解为 $x_1, x_2, \cdots, x_k$（其中可能有相重的），那么，那么 $f(x)$ 一定可以表为

$$f(x) \equiv (x - x_1)(x - x_2)\cdots(x - x_k)g(x) (\bmod p)$$

的形式，其中 $g(x)$ 是一个整系数多项式，$g(x) \equiv 0 (\bmod p)$ 没有解。

反之若多项式 $f(x)$ 可以表为上述形式，那么在素数模 p 下，$f(x)$ 的所有解为（其中可能有相重的）即为 $x_1, x_2, \cdots, x_k$。

定理 3.9.12

(1) 模为素数 p 的 n 次同余式不可能有多于 n 个的对于模 p 不同的根，如果它有 n 个根，则它的左边一定可以在模 p 下分解成为 n 个一次因子；

(2) 如果一个 n 次多项式在素数模 p 下有多于 n 个对模 p 不同的根，那么此多项式必绝对同余于模 p，即 p 可整除它的所有系数。

证明 (1) 假设多项式 $f(x)$ 是 n 次的，但是有 $n+1$ 个对模 p 不同的根。设这些根为 $x_1, x_2, \cdots, x_{n+1}$，于是根据定理 3.9.11 必有

$$f(x) \equiv c(x - x_1)(x - x_2)\cdots(x - x_n)(\bmod p)$$

其中 $(c, p) = 1$，把 x_{n+1} 代入上式得

$$c(x - x_1)(x - x_2)\cdots(x - x_n) \equiv 0 (\bmod p)$$

于是根据 p 是素数，$(c, p) = 1$ 和同余式的性质即得必存在某一个指标 k 使得 $p \mid (x - x_k)$，或者 $x - x_k \equiv 0 (\bmod p)$，这与我们关于 $x_1, x_2, \cdots, x_{n+1}$ 是对模 p 不同的根的假定相矛盾。这就证明了模为素数 p 的 n 次同余式不可能有多于 n 个的对于模 p 不同的根。(1) 的后一部分结论在刚才的证明中也同时证明了。

(2) 如果 $f(x) \equiv 0 (\bmod m)$ 不是绝对同余式，那么它将有多于 n 个对模 p 不同的根，而我们在(1) 中已证明了这是不可能的。

注意：上面这个定理的证明中用到了 p 是素数的假定，因此对于合成模来说，这一定理不一定成立。

例如 $x^2 \equiv 1 (\bmod 8)$ 就有 4 个解 1,3,5,7。

利用上面的定理我们即可证明下面的：

定理 3.9.13（威尔逊定理） 设 p 是一个素数，则

$$(p-1)! + 1 \equiv 0 (\bmod p)$$

证明 当 $p = 2$ 时，定理显然成立。当 $p > 2$ 时，由于 p 的同余类只有 0，1，

威尔逊（Wilson, John, 1741—1793），英国数学家. 生于威斯特摩兰，卒于同地.

2,⋯,$p-1$ 这 p 个，而在这 p 个同余类中共有 1,2,⋯,$p-1$ 这 $p-1$ 个类是与 p 互素的，因此根据欧拉－费马定理，即知 $x^{p-1}-1\equiv 0(\mathrm{mod}\ p)$ 恰有 1,2,⋯,$p-1$ 这 $p-1$ 个根。于是由定理 3.9.12 即得出 $x^{p-1}-1\equiv(x-1)(x-2)\cdots(x-p+1)(\mathrm{mod}\ p)$ 是一个绝对同余式，由此，把 $x=0$ 代入上式并注意当 $p>2$ 时，$p-1$ 一定是一个偶数我们就得到

$$-1\equiv(p-1)!(-1)^{p-1}(\mathrm{mod}\ p)$$

这就证明了定理。

刚才我们研究了在模是素数的情况下同余式的次数和模的一般关系。下面我们进一步研究一下同余式的解数和次数相等的情况。

定理 3.9.14 设 $f(x)=x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n$，$n\leqslant p$，$x^p-x=q(x)f(x)+r(x)$，其中 $q(x)$，$r(x)$ 都是整系数多项式，且 $r(x)$ 的次数小于 n。则 $f(x)\equiv 0(\mathrm{mod}\ p)$ 有 n 个解的充分必要条件是 $r(x)$ 的所有系数都是 p 的倍数。

证明 如果 $f(x)\equiv 0(\mathrm{mod}\ p)$ 有 n 个解，则因为 $n\leqslant p$，且这 n 个解必分别同余于某个小于 p 的整数。于是根据欧拉－费马定理，它们都是 $x^p-x\equiv 0(\mathrm{mod}\ p)$ 的解。因而也都是 $r(x)\equiv 0(\mathrm{mod}\ p)$ 的解。但是由于 $r(x)$ 的次数小于 n，因此由定理 3.9.12 知 $r(x)$ 的所有系数都是 p 的倍数。

反之，如果 $r(x)$ 的所有系数都是 p 的倍数，则由 $x^p-x=q(x)f(x)+r(x)$ 和欧拉－费马定理知，对任何整数 x 都有 $q(x)f(x)\equiv 0(\mathrm{mod}\ p)$。这就是说 $q(x)f(x)\equiv 0(\mathrm{mod}\ p)$ 有 p 个解 $(0,1,2,\cdots,p-1)$。如果 $f(x)\equiv 0(\mathrm{mod}\ p)$ 的解数 $k<n$，那么由定理 3.9.12 知 $p-n$ 次多项式 $q(x)$ 的解数 $h\leqslant p-n$，于是 $q(x)f(x)\equiv 0(\mathrm{mod}\ p)$ 的解数小于等于 $k+h<p$，而这与 $q(x)f(x)\equiv 0(\mathrm{mod}\ p)$ 有 p 个解相矛盾，所得的矛盾就说明 $f(x)\equiv 0(\mathrm{mod}\ p)$ 的解数必等于 n。

综合以上两方面就证明了定理。

例 3.9.8 设 p 是奇素数，证明：$1^2\cdot 3^2\cdot\cdots\cdot(p-2)^2\equiv(-1)^{\frac{p+1}{2}}(\mathrm{mod}\ p)$。

证明

$$\begin{aligned}(p-1)!={}&1\cdot 2\cdot\cdots\cdot(p-1)=\\&(1\cdot 3\cdot\cdots\cdot(p-4)\cdot(p-2))(2\cdot 4\cdot\cdots\cdot(p-3)\cdot(p-1))=\\&(1\cdot 3\cdot\cdots\cdot(p-4)\cdot(p-2))((p-1)\cdot(p-3)\cdot\cdots\cdot 4\cdot 2)=\\&(1\cdot(p-1))\cdot(3\cdot(p-3))\cdot\cdots\cdot((p-4)\cdot 4\cdot)\cdot((p-2)\cdot 2)\equiv\\&(1\cdot(-1))\cdot(3\cdot(-3))\cdot\cdots\cdot((p-4)\cdot(4-p))\cdot\\&(p-2)\cdot(2-p))(\mathrm{mod}\ p)\equiv\\&(-1)^{\frac{p-2}{2}}\cdot 1^2\cdot 3^2\cdot\cdots\cdot(p-2)^2(\mathrm{mod}\ p)\end{aligned}$$

习题 3.9

1. 试解以下问题：

(1) 十一数余 3，七二数余二，十三数余一，问本数；

(2) 二数余一，五数余二，七数余三，九数余四，问本数。(杨辉：续古摘奇算法(1275))

2. (1) 设 m_1, m_2, m_3 是三个正整数，证明：$[(m_1, m_2), (m_2, m_3)] = ([m_1, m_2], m_3)$；

(2) 设 $d = (m_1, m_2)$，证明同余式方程组

$$x \equiv a_1 (\bmod m_1), x \equiv a_2 (\bmod m_2)$$

有解的充分必要条件是 $d \mid (a_1 - a_2)$。且在有解时，其一切解可由下式求出

$$x \equiv x_{1,2} (\bmod [m_1, m_2])$$

其中，$x_{1,2}$ 是同余式方程组 $x \equiv a_1 (\bmod m_1), x \equiv a_2 (\bmod m_2)$ 的一个特解。

(3) 应用(1)，(2) 证明同余式方程组

$$x \equiv a_i (\bmod m_i), i = 1, 2, \cdots, k$$

有解的充分必要条件是 $(m_i, m_j) \mid (a_i, a_j), i, j = 1, 2, \cdots, k$，且在有解时，其一切解可由下式求出：$x \equiv x_{1,2,\cdots,k} (\bmod [m_1, m_2, \cdots, m_k])$，其中，$x_{1,2,\cdots,k}$ 是同余式方程组 $x \equiv a_i (\bmod m_i), i = 1, 2, \cdots, k$ 的一个特解。

3. 设 $m = [m_1, m_2, \cdots, m_k]$。证明

(1) 存在整数 $m'_1, m'_2, \cdots, m'_k$ 两两互素，使得 $m'_i \mid m_i, i = 1, 2, \cdots, k$，且 $m = m'_1 \cdot m'_2 \cdot \cdots \cdot m'_k$；

(2) 同余式方程组 $x \equiv a_i (\bmod m_i), i = 1, 2, \cdots, k$ 的解和同余式方程组 $x \equiv a_i (\bmod m'_i), i = 1, 2, \cdots, k$ 相同。

4. 今有数不知总，以五累减之无剩，以七百十五累减之剩十，以二百四十七累减之剩一百四十，以三百九十一累减之剩二百四十五，以一百八十七累减之剩一百零九，问总数若干？(黄宗宪：求一术通解)

5. 解同余式 $6x^3 + 27x^2 + 17x + 20 \equiv 0 (\bmod 30)$。

6. 解同余式 $31x^4 + 57x^3 + 96x + 191 \equiv 0 (\bmod 225)$。

7. 设 $(a, m) = 1$，x_1 是同余式方程 $ax \equiv 1 (\bmod m)$ 的一个解。再设 k 是正整数，$y_k = 1 - (1 - ax_1)^k$。

证明：(1) $a \mid y_k$；

(2) $x_k = \dfrac{y_k}{a}$ 是同余式方程 $ax \equiv 1 (\bmod m^k)$ 的解。

8. 解同余式方程

(1) $3x \equiv 1 (\bmod 125)$

(2) $5x \equiv 1 \pmod{243}$

9. 求下列二元一次同余式方程组的解

(1) $3x + 4y \equiv 5 \pmod{13}, 2x + 5y \equiv 7 \pmod{13}$

(2) $x + 2y \equiv 1 \pmod 5, 2x + y \equiv 1 \pmod 5$

(3) $x + 3y \equiv 1 \pmod 5, 3x + 4y \equiv 2 \pmod 5$

(4) $4x + y \equiv 2 \pmod 5, 2x + 3y \equiv 1 \pmod 5$

(5) $2x + 3y \equiv 5 \pmod 7, x + 5y \equiv 6 \pmod 5$

(6) $4x + y \equiv 5 \pmod 7, x + 2y \equiv 4 \pmod 7$

10. 设 $m \geqslant 1, \Delta = ad - bc, (m, \Delta) = 1$。那么，二元一次同余式方程组

$$\begin{cases} a_1x + b_1y \equiv c_1 \pmod m \\ a_2x + b_2y \equiv c_2 \pmod m \end{cases}$$

对模 m 有唯一解 $x \equiv \delta(b_2c_1 - b_1c_2) \pmod m, y = \delta(a_1c_2 - a_2c_1) \pmod m$，其中 $\delta\Delta \equiv \pmod m$。

11. 求下列同余式方程的解

(1) $x^3 + 2x - 3 \equiv 0 \pmod{45}$

(2) $4x^2 - 5x + 13 \equiv 0 \pmod{33}$

(3) $x^3 - 9x^2 + 23x - 15 \equiv 0 \pmod{143}$

12. 求下列同余式方程的解

(1) $x^3 + x^2 + 10x + 1 \equiv 0 \pmod{3^3}$

(2) $x^3 + 25x + 3 \equiv 0 \pmod{3^3}$

(3) $x^3 - 5x^2 + 3 \equiv 0 \pmod{3^4}$

(4) $x^5 + x^4 + 1 \equiv 0 \pmod{3^4}$

(5) $x^3 - 2x + 4 \equiv 0 \pmod{5^3}$

(6) $x^3 + x + 57 \equiv 0 \pmod{5^3}$

(7) $x^3 + x^2 - 4 \equiv 0 \pmod{7^3}$

(8) $x^3 + x^2 - 5 \equiv 0 \pmod{7^3}$

(9) $x^2 + 5x + 13 \equiv 0 \pmod{3^3}$

(10) $x^2 + 5x + 13 \equiv 0 \pmod{3^4}$

(11) $x^3 \equiv 3 \pmod{11^3}$

(12) $x^2 \equiv -2 \pmod{19^4}$

13. 求同余式方程 $(x+1)^7 - x^7 - 1 \equiv 0 \pmod{7^7}$ 的满足条件 $7 \nmid x(1+x)$ 的解。

14. 解同余式方程

(1) $x^2 \equiv 2 \pmod{7^k}, k = 5, 6, 7$

(2) $x^2 \equiv -1 \pmod{5^6}$

(3) $x^2 \equiv 4 \pmod{7^4}$

14. 证明:n 是素数的充分必要条件是 $n \mid (n-1)!+1$。

15. 设素数 $p>5$,证明:$(p-1)!+1$ 不可能是素数的方幂。

16. 设 p 是奇素数,证明:

(1) $2^2 \cdot 4^2 \cdot \cdots \cdot (p-1)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$

(2) $\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$

(3) $(p-1)!! \equiv (-1)^{\frac{p-1}{2}}(p-2)!! \pmod{p}$

17. 设 p 为素数,a 为任意整数。证明:

(1) $p \mid a^p+(p-1)!a$

(2) $p \mid (p-1)!a^p+a$

18. 设 p 为奇素数,证明:

(1) 当 $p=4m+3$ 时,对任意 a 均有 $a^2 \not\equiv -1 \pmod{p}$;

(2) 当 $p=4m+1$ 时,必存在一个 a 使得 $a^2 \equiv -1 \pmod{p}$;

(3) 存在无穷多个形如 $4m+1$ 的素数。

3.10 二次同余式

正像在代数中那样,关于同余式方程的结果、理论和应用,大多集中在一次和二次方程中。在代数中,当方程的次数高于二次时,我们甚至都没有一个简明实用的求解公式,而同余式的课题一般来说要比对应的代数方程更复杂,因此可想而知,在高于二次的情况下,它也难于产生更多的东西(不过话又说回来,任何同余式方程的解都是有限的,且不会超过它的模,因此从单纯求解的观点来看,我们甚至不需要任何理论,只要试验下去,总会找出全部解的。但是如果从理论自身发展的内部动力和需要来看,理论还是需要的,而且会产生意想不到的应用)。

二次同余式的一般形状是

$$ax^2+bx+c \equiv 0 \pmod{m},\ a \not\equiv 0 \pmod{m}$$

设 m 的素因子分解式为 $m=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$,则由定理 3.9.5 可知上面的方程与方程组

$$ax^2+bx+c \equiv 0 \pmod{p_i^{\alpha_i}},\ a \not\equiv 0 \pmod{m},\ i=1,2,\cdots,k$$

等价。因此问题化为求解以素数幂为模的同余式方程

$$ax^2+bx+c \equiv 0 \pmod{p^{\alpha}},\ a \not\equiv 0 \pmod{p^{\alpha}}$$

而由 3.9 的讨论,求解这一方程又可化为求解方程

$$ax^2 + bx + c \equiv 0 \pmod p, a \not\equiv 0 \pmod p$$

对 $p = 2$ 的情况，不难讨论。因此不妨设 $p > 2$。这时 $(4a, p) = 1$。用 $4a$ 乘上面的同余式并配方即得

$$(2ax + b)^2 \equiv b^2 - 4ac \pmod p$$

令 $y \equiv 2ax + b \pmod p$ 由于是讨论模 p 的同余式方程，变数替换 $y = 2ax + b$ 和前面的同余式变换是一样的)，我们得到 $y^2 \equiv b^2 - 4ac \pmod p$。如果 $y^2 \equiv b^2 - 4ac \pmod p$ 有一个解 $y \equiv y_0 \pmod p$，那么通过变量替换 $y \equiv 2ax + b \pmod p$ 就得出 $(2ax + b)^2 \equiv b^2 - 4ac \pmod p$ 的一个解 $x \equiv x_0 \pmod p$ (因为 $y \equiv 2ax + b \pmod p$ 可以看成是关于 x 的一次同余式，而由于 $(2a, p) = 1$，因此这个一次同余式有唯一解)。而且当 y_0 不同时，得出的 x_0 也不同(因为 $y \equiv 2ax + b \pmod p$ 的解是唯一的)。反过来从 $(2ax + b)^2 \equiv b^2 - 4ac \pmod p$ 的一个解 $x \equiv x_0 \pmod p$ 通过变换 $y \equiv 2ax + b \pmod p$ 显然可以唯一地确定 $y^2 \equiv b^2 - 4ac \pmod p$ 的一个解 $y \equiv y_0 \pmod p$。由此可见，这两个方程同时有解或无解，且在有解时，解的数目相同，这就得出这两个方程是等价的。

由以上讨论知，最后的问题归结为讨论二次同余式方程

$$x^2 \equiv a \pmod p$$

是否有解。如果 $(a, p) \neq 1$，那么 $(a, p) = p$，即 $p \mid a$，或者 $a \equiv 0 \pmod p$，这时上面的方程显然有唯一解 $x \equiv 0 \pmod p$。因此以下不妨设 $(a, p) = 1$。

先不管方程 $x^2 \equiv a \pmod p$，$(a, p) = 1$ 是否有解，我们首先可以断定以下的事实：

引理 3.10.1 设素数 $p > 2$，a 是整数，且 $(a, p) = 1$。那么方程 $x^2 \equiv a \pmod p$ 恰有两解或无解。

证明 方程 $x^2 \equiv a \pmod p$，$(a, p) = 1$ 可能无解，例如 $x^2 \equiv 2 \pmod 5$ 通过直接检验即可知此方程无解)。

如果方程 $x^2 \equiv a \pmod p$ 有一个解 $x \equiv r \pmod p$，则 $p - r$ 也是一个解，且它不同于 r，否则将有 $r \equiv p - r \pmod p$，$2r \equiv 0 \pmod p$。由于 $(2, p) = 1$，我们得出 $r \equiv 0 \pmod p$，这与 r 是方程 $x^2 \equiv a \pmod p$ 的解的假设相矛盾。

而根据定理3.9.12，方程 $x^2 \equiv a \pmod p$ 至多有两个对模 p 不同的解，因此 r 和 $p - r$ 就是这个方程的全部可能的解。

为此我们引进以下定义：

定义 3.10.1 设素数 $p > 2$，a 是整数。如果同余式方程 $x^2 \equiv a \pmod p$，$(a, p) = 1$ 有解，则称 a 是模 p 的平方剩余，如果同余式方程 $x^2 \equiv a \pmod p$，$(a, p) = 1$ 无解，则称 a 是模 p 的平方非剩余。

根据这个定义，二次同余式方程 $x^2 \equiv a \pmod p$，$(a, p) = 1$ 是否有解的问题就等价于判断整数 a 是否是模 p 的平方剩余。为给出 a 是否是模 p 的平方剩

余的判据，我们首先证明以下引理。

引理 3.10.2 设 p 是一个奇素数，$(a,p)=1$，则

$$a^{\frac{p-1}{2}} \equiv 1 \pmod p$$

或者

$$a^{\frac{p-1}{2}} \equiv -1 \pmod p$$

证明 设 $1<r<p-1$，则必有 $r^2 \not\equiv 1 \pmod p$。假设不然，则 $r \not\equiv \pm 1 \pmod p$，$r^2 \not\equiv 1 \pmod p$。于是 $p \mid (r-1)$ 或者 $p \mid (r+1)$，从而 $r \equiv \pm 1 \pmod p$，这与 $r \not\equiv \pm 1 \pmod p$ 矛盾。所得的矛盾就说明必有 $r^2 \not\equiv 1 \pmod p$。

如果 $a^{\frac{p-1}{2}} \equiv r \pmod p$，$1 \leqslant r < p$，而 $r \neq \pm 1$。那么 $1<r<p-1$，因此 $r^2 \not\equiv 1 \pmod p$。但是把同余式 $a^{\frac{p-1}{2}} \equiv r \pmod p$ 两边平方并利用费马定理又得

$$r^2 \equiv a^{p-1} \pmod p = 1 \pmod p$$

这与 $r^2 \not\equiv 1 \pmod p$ 矛盾。这就说明必有 $r=\pm 1$。

定理 3.10.1(欧拉判别条件) 设 $(a,p)=1$，则 a 是模 p 的平方剩余的充分必要条件是

$$a^{\frac{p-1}{2}} \equiv 1 \pmod p$$

而 a 是模 p 的非平方剩余的充分必要条件是

$$a^{\frac{p-1}{2}} \equiv -1 \pmod p$$

证明 (1) 设 $y=x^2$，则由于

$$(y-a) \mid (y^{\frac{p-1}{2}} - a^{\frac{p-1}{2}})$$

因此可知 $(x^2-a) \mid (x^{p-1} - a^{\frac{p-1}{2}})$ 即存在一个整系数多项式 $q(x)$ 使得 $x^{p-1} - a^{\frac{p-1}{2}} = (x^2-a)q(x)$，故我们有

$$x = x(x^{p-1}-1) = x(x^{p-1} - a^{\frac{p-1}{2}}) + (a^{\frac{p-1}{2}}-1)x =$$
$$(x^2-a)xq(x) + (a^{\frac{p-1}{2}}-1)x$$

从而

$$(x^2-a)xq(x) + (a^{\frac{p-1}{2}}-1)x \equiv (x^p - x) \pmod p \equiv 0 \pmod p$$

如果 a 是平方剩余，则存在一个 r，$(r,p)=1$ 使得 $r^2 \equiv a \pmod p$，$(r^2 - a) \equiv 0 \pmod p$，把此式代入上式即得 $(a^{\frac{p-1}{2}}-1)r \equiv 0 \pmod p$，由于 $(r,p)=1$，故 $(a^{\frac{p-1}{2}}-1) \equiv 0 \pmod p$ 这就说明

$$a^{\frac{p-1}{2}} \equiv 1 \pmod p$$

反之，如果

$$a^{\frac{p-1}{2}} \equiv 1 \pmod p$$

设 $1 \leqslant r \leqslant p-1$，因此 $(r,p)=1$。那么对每一个 r，同余式方程

$$rx \equiv a(\bmod p)$$

有唯一解 $s(r)$。由定理3.7.2知，当 x 遍历 $0,1,\cdots,p-1$ 时，rx 也遍历 $0,1,\cdots,p-1$。由此可知当 $r_1 \neq r_2$ 时，$s(r_1) \neq s(r_2)$。假设对每一个 r，都有 $r \neq s(r)$。那么由于 $p-1$ 是一个偶数，因此必可用 $r \to s(r)$ 的对应方式将 $1,2,\cdots,p-1$ 两两配对，共配成 $\frac{p-1}{2}$ 个对子。将这 $\frac{p-1}{2}$ 个对子连乘起来就得到

$$-1 \equiv (p-1)! \equiv (1s(1))(2s(2))\cdots\left(\frac{p-1}{2}s\left(\frac{p-1}{2}\right)\right) \equiv a^{\frac{p-1}{2}} \equiv 1(\bmod p)$$

显然这是一个矛盾，所得的矛盾说明必存在一个 r 使得 $r = s(r)$，这也就是说

$$r^2 \equiv a(\bmod p)$$

或者说 a 是模 p 的平方剩余。

(2) 由费马定理知，如果 $(a,p)=1$，则 $a^{p-1} \equiv 1(\bmod p)$。因此

$$(a^{\frac{p-1}{2}}+1)(a^{\frac{p-1}{2}}-1) \equiv 0(\bmod p)$$

由于 p 是奇素数，故由引理3.10.2知 $a^{\frac{p-1}{2}} \equiv 1(\bmod p)$ 和 $a^{\frac{p-1}{2}} \equiv -1(\bmod p)$ 这两个式子之中必有一个式子成立且二式不可能同时成立，但是在(1)中已证明 a 不是平方剩余的充分必要条件是 $a^{\frac{p-1}{2}} \not\equiv 1(\bmod p)$，故 a 是平方非剩余的充分必要条件就是 $a^{\frac{p-1}{2}} \equiv -1(\bmod p)$。

现在来看看在 $1,2,\cdots,p-1$ 这 $p-1$ 个数中有多少个数是平方剩余，有多少个数是平方非剩余。由于平方剩余数和平方非剩余数是完全对称的概念，所以从直觉上说，我们感觉到这两种数应该是一样多的。不过这当然不能算是证明，下面我们就来严格证明这一结论。

定理3.10.2 设 p 是一个奇素数，则在 $1,2,\cdots,p-1$ 这 $p-1$ 个数中平方剩余数和平方非剩余数的个数各为 $\frac{p-1}{2}$。而且 $\frac{p-1}{2}$ 个平方剩余数分别与 1^2，$2^2,\cdots,\left(\frac{p-1}{2}\right)^2$ 中的一个数同余，且仅与一个数同余。

证明 显然当 a 同余于 $1^2,2^2,\cdots,\left(\frac{p-1}{2}\right)^2$ 中的某一个数时，a 必定是一个平方剩余。由于 $-k \equiv p-k(\bmod p)$，所以

$$1^2 \equiv (-1)^2 \equiv (p-1)^2(\bmod p), 2^2 \equiv (p-2)^2, \cdots,$$

$$\left(\frac{p-1}{2}\right)^2 \equiv \left(p-\frac{p-1}{2}\right)^2 \equiv \left(\frac{p+1}{2}\right)^2$$

所以 $1^2,2^2,\cdots,\left(\frac{p-1}{2}\right)^2$ 就是 $1,2,\cdots,p-1$ 这 $p-1$ 个数中所有可能的平方剩余数了。

当 $x \equiv \pm i, \pm j(\bmod p)$。$1 \leqslant i < j \leqslant \frac{p-1}{2}$ 时，$i^2 \not\equiv j^2(\bmod p)$。否则二次

同余式方程 $x^2 \equiv i^2 (\bmod\ p)$ 将有 4 个解，而这与引理 3.10.1 矛盾，因此在 1，2，…，$p-1$ 这 $p-1$ 个数中恰有 $\frac{p-1}{2}$ 个平方剩余数，且每一个平方剩余数都与 $1^2, 2^2, \cdots, \left(\frac{p-1}{2}\right)^2$ 中的某一个数同余，且仅与一个数同余。而剩下的 $\frac{p-1}{2}$ 个数就是平方非剩余数。

例 3.10.1　求模 11 的平方剩余与平方非剩余。

解　根据定理 3.10.2 求模 11 的平方剩余数为 $1^2 \equiv 1, 2^2 \equiv 4, 3^2 \equiv 9, 4^2 \equiv 16 \equiv 5, 5^2 \equiv 25 \equiv 3 (\bmod\ 11)$，即 1，3，4，5，9，而平方非剩余数就是 2，6，7，8，10。

例 3.10.2　求模 29 的平方剩余与平方非剩余。

解　求法和例 3.10.1 相同，但是可列出下表使表达更简明：

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$i^2 (\bmod\ 29)$	1	4	9	16	25	7	20	6	23	13	5	28	24	22

故模 29 的平方剩余就是 1，4，5，6，7，9，13，16，20，22，23，24，25，28；而平方非剩余就是 2，3，8，10，11，12，14，15，17，18，19，21，26，27。

由上表不仅可以得到模 p 的平方剩余，还可以查出当 a 是模 p 的平方剩余时，二次同余式方程的 $x^2 \equiv a (\bmod\ p)$ 的两个解。例如 25 是模 29 的平方剩余，因此的两个解是 $x^2 \equiv 25 (\bmod\ 29)$ 的两个解是 $x \equiv 5, 29-5 \equiv 5, 24 (\bmod\ 29)$。

例 3.10.3　设 p 是一个奇素数，则 -1 是模 p 的平方剩余的充分必要条件是 $p \equiv 1 (\bmod\ 4)$；当 $p \equiv 1 (\bmod\ 4)$ 时，二次同余式方程 $x^2 \equiv -1 (\bmod\ p)$ 的解是

$$x \equiv \pm \left(\frac{p-1}{2}\right)!$$

证明　由欧拉判别条件知 -1 是模 p 的平方剩余的充分必要条件是

$$(-1)^{\frac{p-1}{2}} \equiv 1 (\bmod\ p)$$

上述条件等价于 $(-1)^{\frac{p-1}{2}} = 1$，这一条件又等价于 $\frac{p-1}{2}$ 是偶数或 $p \equiv 1 (\bmod\ 4)$；$p \equiv 1 (\bmod\ 4)$ 时，由于在模 p 下 $p-1 \equiv -1, p-2 \equiv -2, \cdots, p-(p-1) \equiv -(p-1)$，因此

$$\begin{aligned}
-1 \equiv (p-1)! \equiv & (-1)(-2)\cdots(-(p-1)) \equiv \\
& ((-1)(-(p-1)))((-2)(-(p-2)))\cdots \\
& \left(\left(-\frac{p-1}{2}\right)\left(-\left(p-\frac{p-1}{2}\right)\right)\right) \equiv \\
& (-1 \cdot 1)(-2 \cdot 2)\cdots\left(-\frac{p-1}{2} \cdot \frac{p-1}{2}\right) \equiv \\
& (-1)^{\frac{p-1}{2}}\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv \\
& \left(\left(\frac{p-1}{2}\right)!\right)^2
\end{aligned}$$

由此即得二次同余式方程 $x^2 \equiv -1 \pmod p$ 的解是 $x \equiv \pm\left(\frac{p-1}{2}\right)!$。

欧拉判别条件虽然给出了判别一个数是否是模 p 的平方剩余的判据，但是直接应用这一法则去判别却并不方便。但是这一判据把判别问题化为了计算，而且只须关系结果的符号，这就隐含了某种简化的原则，而这一简化需要通过一套符号系统来实现(这里顺便提一下，一套好的符号系统有助于理清我们的思路，使我们的思维集中到问题的最本质的方面去，因此在数学研究中的作用是很重要的，而我国古代的数学虽然曾经取得过辉煌的成就，但是到了中近代，却落后于西方(不仅是数学) 科学的发展，其中一个原因就在于我国古代的数学没有一套很好的符号系统，结果使得我国古代的数学研究的表达十分繁琐晦涩，难于为普通人所掌握，另一个原因在于我国古代的统治阶级从来不重视科学的研究，只把它看成一种神秘的东西或好玩的东西或只看重它的实用性而不重视其本身的基础和系统的发展，研究科学的人也一直被视为与道士、巫师、艺人一类的下九流的小玩意)。下面我们就来介绍这一套符号系统。

勒让德(Legendre, Adrien-Marie, 1752—1833)，法国数学家，生于巴黎(另一说为图卢兹)，卒于巴黎.

定义 3.10.2 勒让德符号 $\left(\frac{a}{p}\right)$ 的意义如下：当 a 是模 p 的平方剩余时，$\left(\frac{a}{p}\right)=1$，当 a 是模 p 的平方非剩余时，$\left(\frac{a}{p}\right)=-1$，当 $p \mid a$ 时，$\left(\frac{a}{p}\right)=0$。

于是平方剩余的判别问题现在就化为了勒让德符号的计算问题。为能简便地计算勒让德符号，首先需要研究它的性质。由定义容易直接证明下面的

引理 3.10.3 设 p 是奇素数，那么勒让德符号有以下性质：

(1) $\left(\frac{a}{p}\right) = (-1)^{\frac{p-1}{2}} \pmod p$；

(2) 如果 $a \equiv b \pmod p$，则 $\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$；

(3) $\left(\frac{1}{p}\right)=1$，$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$；或者

当 $p \equiv 1 \pmod 4$ 时，$\left(\frac{-1}{p}\right)=1$，当 $p \equiv 3 \pmod 4$ 时，$\left(\frac{-1}{p}\right)=-1$。

(4) $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$；

(5) 当 $p \nmid a$ 时，$\left(\frac{a^2}{p}\right)=1$。

下面一个引理就不像上面那样直观和容易了。

引理 3.10.4(高斯引理) 设 p 为奇素数，$p \nmid a$。又设在

$$a, 2a, \cdots, \left(\frac{p-1}{2}\right)a$$

被 p 除所得的余数中，恰有 m 个大于 $\frac{p-1}{2}$，则

(1) $\left(\frac{a}{p}\right) = (-1)^m$；

(2) $m \equiv \sum_{k=1}^{\frac{p-1}{2}}\left[\frac{ka}{p}\right] - (a-1)\frac{p^2-1}{8}\pmod 2$。

证明 (1) 设 $r_1, r_2, \cdots, r_n$ 表示在 $a, 2a, \cdots, \left(\frac{p-1}{2}\right)a$ 被 p 除所得的余数中，小于或者等于 $\frac{p-1}{2}$ 的数；又设 $s_1, s_2, \cdots, s_m$ 表示在 $a, 2a, \cdots, \left(\frac{p-1}{2}\right)a$ 被 p 除所得的余数中，大于 $\frac{p-1}{2}$ 的数，那么显然 $n + m = \frac{p-1}{2}$。

首先证明，任意两个 r_i 在模 p 下都不会同余，否者将有 $0 \leqslant x_1 \leqslant \frac{p-1}{2}, 0 \leqslant x_2 \leqslant \frac{p-1}{2}$ 使得 $ax_1 = q_1p + r_1, ax_2 = q_2p + r_2$。由 $r_1 \equiv r_2 \pmod p$ 得出 $ax_1 \equiv ax_2 \pmod p$，由于 $(a, p) = 1$，故得出 $x_1 \equiv x_2 \pmod p$，$x_1 = x_2$。这与 $x_1 \neq x_2$ 矛盾。同理，任何两个 s_i 在模 p 下也不会同余。

现在我们再证明，对任意 i 和 j，$r_i \not\equiv p - s_j \pmod p$。假设不然，则有 $r_i \equiv p - s_j \pmod p$，$r_i + s_j \equiv 0 \pmod p$。又因为 $r_i \equiv ta \pmod p$，$s_j \equiv ua \pmod p$，其中 t 和 u 是小于或者等于 $\frac{p-1}{2}$ 的两个正整数，这就得出 $(t+u)a \equiv 0 \pmod p$，因为 $(a, p) = 1$，因而就得出 $t + u \equiv 0 \pmod p$，但因为 $2 \leqslant t + u \leqslant p - 1$，所以这是不可能的。所得的矛盾就证明了对任意 i 和 j，$r_i \not\equiv p - s_j \pmod p$。

于是，$r_1, r_2, \cdots, r_n$ 和 $p - s_1, p - s_2, \cdots, p - s_m$ 这 $\frac{p-1}{2}$ 个两两不同的且都不大于 $\frac{p-1}{2}$ 的数显然就构成 $1, 2, \cdots, \frac{p-1}{2}$ 的一个排列，因此就有

$$r_1r_2\cdots r_n(p - s_1)(p - s_2)\cdots(p - s_m) = 1 \cdot 2 \cdot \cdots \cdot \left(\frac{p-1}{2}\right) = \left(\frac{p-1}{2}\right)!$$

由于对所有的 j 成立 $p - s_j \equiv -s_j \pmod p$，而这种因子共有 m 个，因而上式就成为

$$r_1r_2\cdots r_ns_1s_2\cdots s_m(-1)^m \equiv \left(\frac{p-1}{2}\right)! \pmod p$$

但是按照 $r_1, r_2, \cdots, r_n$ 和 $s_1, s_2, \cdots, s_m$ 的定义，这 $\frac{p-1}{2}$ 个数都是 $a, 2a\cdots, \left(\frac{p-1}{2}\right)a$ 这 $\frac{p-1}{2}$ 个数除以 p 所得的余数，因此它们之中的每一个数都与 $a, 2a, \cdots, \left(\frac{p-1}{2}\right)a$ 中的某一个数同余，因此在模 p 下乘积 $r_1r_2\cdots r_ns_1s_2\cdots s_m(-1)^m$ 与乘积 $a \cdot 2a \cdot \cdots \cdot \left(\frac{p-1}{2}\right)a \cdot (-1)^m$ 同余。故由前面已证的式子就得出

$$(-1)^m a^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)! \equiv \left(\frac{p-1}{2}\right)!(\bmod p)$$

在这个式子中$\left(\frac{p-1}{2}\right)!$的每个因子都与 p 互素因而可以消去，把它们消去后即得

$$(-1)^m a^{\frac{p-1}{2}} \equiv (\bmod p)$$

在上式两边都乘以$(-1)^m$ 后即得 $a^{\frac{p-1}{2}} \equiv (-1)^m(\bmod p)$。再利用 $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)(\bmod p)$ 就最后得到

$$\left(\frac{a}{p}\right) = (-1)^m$$

这就证明了(1)。

(2) 由带余数除法知 $ka = qp + r$，其中 $q = \left[\frac{ka}{p}\right]$。又

$$1 + 2 + \cdots + \frac{p-1}{2} = \left(1 + \frac{p-1}{2}\right) \cdot \frac{p-1}{4} = \frac{p^2-1}{8}$$

所以 $$a\frac{p^2-1}{8} = a + 2a + \cdots + \frac{p-1}{2}a =$$

$$p\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{ka}{p}\right] + r_1 + r_2 + \cdots + r_n + s_1 + s_2 + \cdots + s_m =$$

$$p\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{ka}{p}\right] + \sum_{i=1}^{n} r_i + \sum_{j=1}^{m}(p - s_j) - mp + 2\sum_{j=1}^{m} s_j$$

其中 $r_1, r_2, \cdots, r_n$ 和$s_1, s_2, \cdots, s_m$ 分别表示 $a, 2a, \cdots, \left(\frac{p-1}{2}\right)a$ 这$\frac{p-1}{2}$ 个数除以 p 所得的余数中小于等于$\frac{p-1}{2}$ 的数和大于$\frac{p-1}{2}$ 的数。在(1) 中已说明 $r_1, r_2, \cdots, r_n$ 和$p - s_1, p - s_2, \cdots, p - s_m$ 这$\frac{p-1}{2}$个两两不同的且都不大于$\frac{p-1}{2}$的数构成 $1, 2, \cdots, \frac{p-1}{2}$ 的一个排列，因此

$$\sum_{i=1}^{n} r_i + \sum_{j=1}^{m}(p - s_j) = \sum_{k=1}^{\frac{p-1}{2}} k = \frac{p^2-1}{8}$$

把此式代入上面的式子就得到

$$(a-1)^{\frac{p^2-1}{8}} = p\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{ka}{p}\right] - mp + 2\sum_{j=1}^{m} s_j \equiv$$

$$1\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{ka}{p}\right] - m \cdot 1(\bmod 2)$$

定理 3.10.3

(1)
$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$$
因而当 $p\equiv 1,7(\bmod 8)$ 时，$\left(\frac{2}{p}\right)=1$；当 $p\equiv 3,5(\bmod 8)$ 时，$\left(\frac{2}{p}\right)=-1$；

(2) 如果 $(a,p)=1, 2\nmid a$，则 $\left(\frac{a}{p}\right)=(-1)^{\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{ka}{p}\right]}$。

证明 (1) 当 $a=2$ 时，$0\leqslant\left[\frac{ka}{p}\right]\leqslant\left[\frac{2k}{p}\right]\leqslant\left[\frac{p-1}{p}\right]\leqslant 0$，因而由引理 3.10.4 就得到
$$m\equiv\frac{p^2-1}{8}(\bmod 2)$$
再由引理 3.10.3 和引理 3.10.4 就得到 $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$；

(2) 如果 $(a,p)=1, 2\nmid a$，则 $a-1\equiv 0(\bmod 2)$，因此引理 3.10.4(2) 就得到
$$\left(\frac{a}{p}\right)=(-1)^{\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{ka}{p}\right]}$$
定理 3.10.4(二次互反律) 设 p,q 都是奇素数，且 $(p,q)=1$，则
$$\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right)$$
证明 由定理 3.8.4 和定理 3.10.3 就得到
$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\sum_{k=1}^{\frac{q-1}{2}}\left[\frac{kq}{p}\right]+\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{hq}{p}\right]}=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$
在上式两边同乘以 $\left(\frac{p}{q}\right)$ 就得到定理。

例 3.10.4 计算 $\left(\frac{438}{593}\right)$。

解 先把分子 438 分解成素因数的乘积：$438=2\cdot 3\cdot 73$，因此
$$\left(\frac{438}{593}\right)=\left(\frac{2}{593}\right)\left(\frac{3}{593}\right)\left(\frac{73}{593}\right)=\left(\frac{3}{593}\right)\left(\frac{73}{593}\right)=$$
$$\left(\frac{593}{3}\right)\left(\frac{593}{73}\right)=\left(\frac{2}{3}\right)\left(\frac{9}{73}\right)=\left(\frac{2}{3}\right)=-1$$
因此同余式方程 $x^2\equiv 438(\bmod 593)$ 无解。

这个例子也可以用 $438\equiv -155(\bmod 593)$，$155=5\cdot 31$ 去做。由于 $\left(\frac{-1}{593}\right)=1$，所以
$$\left(\frac{438}{593}\right)=\left(\frac{-155}{593}\right)=\left(\frac{-1}{593}\right)\left(\frac{5}{593}\right)\left(\frac{31}{593}\right)=\left(\frac{5}{593}\right)\left(\frac{31}{593}\right)=$$

$$\left(\frac{593}{5}\right)\left(\frac{593}{31}\right)=\left(\frac{3}{5}\right)\left(\frac{4}{31}\right)=\left(\frac{5}{3}\right)=\left(\frac{2}{3}\right)=-1$$

例 3.10.5 计算$\left(\frac{2\,023}{1\,231}\right)$。

解 $$\left(\frac{2\,023}{1\,231}\right)=\left(\frac{792}{1\,231}\right)=\left(\frac{2^3}{1\,231}\right)\left(\frac{3^2}{1\,231}\right)\left(\frac{11}{1\,231}\right)=\left(\frac{2}{1\,231}\right)\left(\frac{11}{1\,231}\right)=$$
$$\left(\frac{11}{1\,231}\right)=-\left(\frac{1\,231}{11}\right)=-\left(\frac{-1}{11}\right)=1$$

故同余式方程 $x^2\equiv 2\,023(\bmod 1\,231)$ 有解。

虽然勒让德符号已能够在实际计算中应用，但是在计算过程中需要运用互反律时，必须将符号上方分解成素因数的乘积，而这是没有一般方法的，因此这个方法对实际计算来说，在一定程度上还是有缺点的。为去掉这个缺点，我们还要进一步引进所谓雅可比符号。

雅可比(Jacobi, Carl Gustav Jacob, 1804—1851)，德国数学家，生于波茨坦，卒于柏林。

定义 3.10.3 设 P 是一个大于 1 的奇数，$P=p_1p_2\cdots p_k$ 是 P 的素因子分解式(这其中可以有相同的)。$(a,P)=1$，则雅可比符号$\left(\frac{a}{p}\right)$(读作 a 对 P 的雅可比符号) 的意义为

$$\left(\frac{a}{p}\right)=\left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_k}\right)$$

其中$\left(\frac{a}{p_i}\right)$表示 a 对 p_i 的勒让德符号。

显然，当 P 本身是奇素数时，雅可比符号就是勒让德符号，所以雅可比符号是勒让德符号的一种推广。由定义和勒让德符号的基本性质立即推出雅可比符号的下述性质：

引理 3.10.5 雅可比符号有以下性质：

(1) $\left(\frac{1}{P}\right)=1$；当 $a\mid P$ 时，$\left(\frac{a}{P}\right)=0$；当$(a,P)=1$时，$\left(\frac{a}{P}\right)=1$或者 -1；

(2) 如果 $a\equiv b(\bmod P)$，则$\left(\frac{a}{P}\right)=\left(\frac{b}{P}\right)$；

(3) $\left(\frac{ab}{P}\right)=\left(\frac{a}{P}\right)\left(\frac{b}{P}\right)$；

(4) $\left(\frac{a}{PQ}\right)=\left(\frac{a}{P}\right)\left(\frac{b}{Q}\right)$；

(5) 当$(a,P)=1$时，$\left(\frac{a^2}{P}\right)=\left(\frac{b}{P^2}\right)=1$。

为得出雅可比符号的进一步的性质，首先证明下面的引理；

引理 3.10.6 设$2\nmid P$，$P=p_1p_2\cdots p_k$ 是P 的素因子分解式(这其中可以有相同的)，则

(1) $\frac{P-1}{2}=\frac{p_1-1}{2}+\frac{p_2-1}{2}+\cdots+\frac{p_k-1}{2}+2N$；

(2) $\frac{P^2-1}{8}=\frac{p_1^2-1}{8}+\frac{p_2^2-1}{8}+\cdots+\frac{p_k^2-1}{8}+2M$。

其中，M 和 N 都是整数。

证明

(1) $\frac{P-1}{2}=\frac{p_1p_2\cdots p_k-1}{2}=$

$$\left(\frac{1}{2}\right)\left(\left(1+2\frac{p_1-1}{2}\right)\left(1+2\frac{p_2-1}{2}\right)\cdots\left(1+2\frac{p_k-1}{2}\right)-1\right)=$$

$$\frac{p_1-1}{2}+\frac{p_2-1}{2}+\cdots+\frac{p_k-1}{2}+2N$$

(2) $\frac{P^2-1}{8}=\frac{p_1^2p_2^2\cdots p_k^2-1}{8}=$

$$\left(\frac{1}{8}\right)\left(\left(1+8\frac{p_1^2-1}{8}\right)\left(1+8\frac{p_2^2-1}{8}\right)\cdots\left(1+8\frac{p_k^2-1}{8}\right)-1\right)=$$

$$\frac{p_1^2-1}{8}+\frac{p_2^2-1}{8}+\cdots+\frac{p_k^2-1}{8}+2M$$

定理 3.10.5

(1) $\left(\frac{-1}{P}\right)=(-1)^{\frac{P-1}{2}}$；

(2) $\left(\frac{2}{P}\right)=(-1)^{\frac{P^2-1}{8}}$。

证明 (1) 由引理 3.10.5 和引理 3.10.6 即得

$$\left(\frac{-1}{P}\right)=\left(\frac{-1}{p_1}\right)\left(\frac{-1}{p_2}\right)\cdots\left(\frac{-1}{p_k}\right)=(-1)^{\frac{p_1-1}{2}}(-1)^{\frac{p_2-1}{2}}\cdots(-1)^{\frac{p_k-1}{2}}=$$

$$(-1)^{\frac{p_1-1}{2}+\frac{p_2-1}{2}+\cdots+\frac{p_k-1}{2}}=(-1)^{\frac{P-1}{2}-2N}=(-1)^{\frac{P-1}{2}}$$

(2) $$\left(\frac{2}{P}\right)=\left(\frac{2}{p_1}\right)\left(\frac{2}{p_2}\right)\cdots\left(\frac{2}{p_k}\right)=(-1)^{\frac{p_1^2-1}{8}}(-1)^{\frac{p_2^2-1}{8}}\cdots(-1)^{\frac{p_k^2-1}{8}}=$$

$$(-1)^{\frac{p_1^2-1}{8}+\frac{p_2^2-1}{8}+\cdots+\frac{p_k^2-1}{8}}=(-1)^{\frac{P^2-1}{8}-2M}=(-1)^{\frac{P^2-1}{8}}$$

定理 3.10.6 设 P,Q 都是大于 1 的奇数，则

$$\left(\frac{Q}{P}\right)=(-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}\left(\frac{P}{Q}\right)$$

证明 如果 $(P,Q)>1$，则 $\left(\frac{Q}{P}\right)=\left(\frac{P}{Q}\right)=0$，因此定理成立。如果 $(P,Q)=1$，那么可设 $Q=q_1q_2\cdots q_s$ 是 Q 的素因子分解式。由定义和引理 3.10.5 以及勒让德符号的二次互反律即得

$$\left(\frac{Q}{P}\right)=\prod_{i=1}^{k}\left(\frac{Q}{p_i}\right)=\prod_{i=1}^{k}\prod_{j=1}^{s}\left(\frac{q_j}{p_i}\right)=\prod_{i=1}^{k}\prod_{j=1}^{s}(-1)^{\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}}\left(\frac{p_i}{q_j}\right)=$$

$$(-1)^{\sum_{i=1}^{k}\sum_{j=1}^{s}\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}}\prod_{i=1}^{k}\prod_{j=1}^{s}\left(\frac{p_i}{q_j}\right)$$

但是由引理 3.10.6 得到

$$\sum_{i=1}^{k}\sum_{j=1}^{s}\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}=\left(\sum_{i=1}^{k}\frac{p_i-1}{2}\right)\left(\sum_{j=1}^{s}\frac{q_j-1}{2}\right)=$$
$$\left(\frac{P-1}{2}+2N_1\right)\left(\frac{Q-1}{2}+2N_2\right)=$$
$$\frac{P-1}{2}\cdot\frac{Q-1}{2}+2N$$

故由此就得到

$$\left(\frac{Q}{P}\right)=(-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}\prod_{i=1}^{k}\prod_{j=1}^{s}\left(\frac{p_i}{q_j}\right)=(-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}\left(\frac{P}{Q}\right)$$

至此,我们可以看出雅可比符号的性质几乎和勒让德符号一样,却没有 P 必须是素数的限制,这就是它的好处。这使我们在计算勒让德符号时可以把它就看成是雅可比符号,这样在实际计算时就比不引进雅可比符号方便许多。

但是我们指出,雅可比符号和勒让德符号有一个重大差别,那就是根据勒让德符号的值可以判断一个二次同余式方程是否有解,然而雅可比符号一般来说却没有这个功能。例如根据定义计算下面的雅可比符号可得出

$$\left(\frac{2}{9}\right)=\left(\frac{2}{3}\right)\left(\frac{2}{3}\right)=1$$

但是同余式方程 $x^2\equiv 2(\bmod 9)$ 却没有解。

例 3.10.6 判断同余式 $x^2\equiv 286(\bmod 563)$ 是否有解。

解 由于 563 是一个奇素数,所以可以用勒让德符号来判别

$$\left(\frac{286}{563}\right)=\left(\frac{2}{563}\right)\left(\frac{143}{563}\right)=(-1)(-1)^{\frac{143-1}{2}\cdot\frac{563-1}{2}}\left(\frac{563}{143}\right)=$$
$$\left(\frac{-9}{143}\right)=\left(\frac{-1}{143}\right)=-1$$

故上述同余式方程无解。

以上我们讨论了当模是奇素数时的二次同余式方程是否有解的判别问题。现在来考虑模是复合数的情况。

设 m 是一个正整数,那么由算术基本定理知可把 m 分解成素因数的乘积

$$m=2^{a}p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}$$

又由定理 3.9.4 知同余式方程 $x^2\equiv a(\bmod m)$ 与同余式方程组

$$x^2\equiv a(\bmod 2^{a}),x^2\equiv a(\bmod p_i^{a_i}),i=1,2,\cdots,k$$

同解,并且在有解的情况下,前者的解数是同余式方程组中各式的解数的乘积。因此问题归结为讨论上述同余式方程组中各式的解,实际上,在上面的同余式方程组中本质上不同的方程只有两种,我们先讨论同余式方程

$$x^2 \equiv a(\bmod p^{\alpha}), a > 0, (a,p) = 1$$

定理 3.10.7 同余式方程 $x^2 \equiv a(\bmod p^{\alpha}), a > 0, (a,p) = 1$ 有解的充分必要条件是

$$\left(\frac{a}{p}\right) = 1$$

如果上面的方程有解，则它有两个解。

证明 如果$\left(\frac{a}{p}\right) = -1$，则同余式方程 $x^2 \equiv a(\bmod p)$ 无解，因此同余式方程 $x^2 \equiv a(\bmod p^{\alpha})$ 无解，故定理中的条件是必要的。

如果$\left(\frac{a}{p}\right) = 1$，则由引理 3.10.1 和勒让德符号的定义知同余式方程 $x^2 \equiv a(\bmod p)$ 恰有两解。设 $x \equiv r(\bmod p)$ 是它的一个解，那么由 $(a,p) = 1$ 得出 $(r,p) = 1$。又因为 $2 \nmid p$，故 $(2r,p) = 1$。令 $f(x) = x^2 - a$，则 $p \nmid f'(r)$，由定理 3.9.10 知从 $x \equiv r(\bmod p)$ 可以得出 $x^2 \equiv a(\bmod p^{\alpha})$ 的一个唯一解，因此由 $x^2 \equiv a(\bmod p)$ 的两个解可以获得 $x^2 \equiv a(\bmod p^{\alpha})$ 的两个解，并且只有两个。这就证明了定理。

现在来讨论同余式方程 $x^2 \equiv a(\bmod 2^{\alpha}), \alpha > 0, (a,2) = 1$。

首先我们立刻可以看出当 $\alpha = 1$ 时，此方程永远有解，并且解数为 1，所以以下总是设 $\alpha > 1$。

定理 3.10.8 设 $\alpha > 1$，则

(1) 当 $\alpha = 2$ 时，同余式方程 $x^2 \equiv a(\bmod 2^{\alpha}), (a,2) = 1$ 有解的必要条件是 $a \equiv 1(\bmod 4)$；

(2) 当 $\alpha \geqslant 3$ 时，同余式方程 $x^2 \equiv a(\bmod 2^{\alpha}), (a,2) = 1$ 有解的必要条件是 $a \equiv 1(\bmod 8)$。

如果上述条件满足，则同余式方程 $x^2 \equiv a(\bmod 2^{\alpha}), \alpha > 1, (a,2) = 1$ 有解，并且当 $\alpha = 2$ 时，解数是 2；当 $\alpha \geqslant 3$ 时，解数是 4。

证明 如果 $x \equiv r(\bmod 2^{\alpha})$ 是 $x^2 \equiv a(\bmod 2^{\alpha})$ 的任一解，那么由 $(a,2) = 1$ 就得出 $(r,2) = 1$。因此 $r = 1 + 2t$，其中 t 是一个整数，由此即得

$$a \equiv r^2 \equiv 1 + 4t(t+1)(\bmod 2^{\alpha})$$

(1) 当 $\alpha = 2$ 时，$2^{\alpha} = 4$，因此 $a \equiv r^2 \equiv 1 + 4t(t+1)(\bmod 4) \equiv 1(\bmod 4)$；

(2) 当 $\alpha \geqslant 3$ 时，2^{α} 是 8 的倍数，故 $a \equiv r^2 \equiv 1 + 4t(t+1)(\bmod 8) \equiv 1(\bmod 8)$。

这就证明了定理中条件的必要性。

当 $\alpha = 2$ 时，如果 $a \equiv 1(\bmod 4)$，则 $a \equiv 1(\bmod 2^{\alpha})$。于是显然 $x \equiv 1,3 (\bmod 2^{\alpha})$ 都是 $x^2 \equiv a(\bmod 2^{\alpha})$ 的解，且仅有这两个解。

当 $\alpha = 3$ 时，如果 $a \equiv 1(\bmod 8)$，则 $a \equiv 1(\bmod 2^{\alpha})$。于是显然 $x \equiv 1,3,5,$

$7 \pmod{2^\alpha}$ 都是 $x^2 \equiv a \pmod{2^\alpha}$ 的解，且仅有这四个解。

当 $\alpha > 3$ 时，如果 $a \equiv 1 \pmod 8$，由刚才的讨论已知适合 $x^2 \equiv a \pmod{2^3}$ 的解是所有的奇数。易于验证所有的奇数都可以写成 $\pm(1 + 4t_3)$，$t_3 = 0, \pm 1, \pm 2, \cdots$ 的形式，我们看在这些数中，哪些适合同余式 $x^2 \equiv a \pmod{16}$，把 $x = \pm(1 + 4t_3)$ 代入这个同余式得 $(1 + 4t_3)^2 \equiv a \pmod{16}$，由此得出

$$t_3 \equiv \frac{a-1}{8} \pmod 2$$

或者

$$t_3 = \frac{a-1}{8} + 2t_4$$

也就是

$$x = \pm 1(1 + 4t'_3 + 8t_4) = \pm(x_4 + 8t_4)$$

其中 $t'_3 = \dfrac{a-1}{8}$，故

$$x \equiv \pm(x_4 + 8t_4),\ x_4 = 1 + 4t'_3,\ t_4 = 0, \pm 1, \pm 2, \cdots$$

是适合同余式 $x^2 \equiv a \pmod{16}$ 的一切整数。用同样的方法可以证明适合同余式 $x^2 \equiv a \pmod{2^5}$ 的一切整数是 $x \equiv \pm(x_5 + 16t_5)$，$x_5^2 \equiv a \pmod{2^5}$，$t_5 = 0, \pm 1, \pm 2, \cdots$。依次类推即可得出对任一 $\alpha > 3$，适合同余式 $x^2 \equiv a \pmod{2^\alpha}$ 的一切整数是 $x \equiv \pm(x_\alpha + 2^{\alpha-1}t_\alpha)$，$x_\alpha^2 \equiv a \pmod{2^\alpha}$，$t_\alpha = 0, \pm 1, \pm 2, \cdots$。这些 x 对模 2^α 来说构成 4 个同余类，即 $x \equiv \pm x_\alpha, \pm(x_\alpha + 2^{\alpha-1}) \pmod{2^\alpha}$。这就是同余式方程 $x^2 \equiv a \pmod{2^\alpha}$ 的全部解。

由以上两个定理即得到

定理 3.10.9 同余式方程 $x^2 \equiv a \pmod m$，$m = 2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$，$(a, m) = 1$ 有解的必要条件为：当 $\alpha = 2$ 时，$a \equiv 1 \pmod 4$；当 $\alpha \geqslant 3$ 时，$a \equiv 1 \pmod 8$ 并且 $\left(\dfrac{a}{p_i}\right) = 1$，$i = 1, 2, \cdots, k$。

如果上述条件成立，则同余式方程 $x^2 \equiv a \pmod m$ 有解。并且当 $\alpha = 0$ 或 1 时，解数是 2^k；当 $\alpha = 2$ 时，解数是 2^{k+1}；当 $\alpha \geqslant 3$ 时，解数是 2^{k+2}。

习题 3.10

1. 用欧拉判别法确定

(1) 在 2,3,5 这三个数中，哪个数是模 13 的平方剩余，哪些数是平方非剩余？

(2) 在 5,7,8 这三个数中，哪个数是模 17 的平方剩余，哪些数是平方非剩余？

2. 计算勒让德符号

(1) $\left(\dfrac{94}{109}\right)$ (2) $\left(\dfrac{111}{271}\right)$ (3) $\left(\dfrac{342}{677}\right)$ (4) $\left(\dfrac{93}{131}\right)$ (5) $\left(\dfrac{2\,115}{6\,269}\right)$ (6) $\left(\dfrac{589}{1283}\right)$

3. 计算以下符号

(1) $\left(\frac{47}{125}\right)$ (2) $\left(\frac{5\,610}{6\,649}\right)$ (3) $\left(\frac{131}{283}\right)$ (4) $\left(\frac{116}{397}\right)$ (5) $\left(\frac{328}{625}\right)$

4. 求数 p 的所有平方剩余

(1) $p = 11$ (2) $p = 13$ (3) $p = 17$ (4) $p = 19$

5. 解同余式

(1) $x^2 \equiv 19 \pmod{31}$ (2) $x^2 \equiv 15 \pmod{53}$

(3) $x^2 \equiv 11 \pmod{59}$ (4) $x^2 \equiv 3 \pmod{37}$

6. 解同余式

(1) $x^2 \equiv 65 \pmod{101}$ (2) $x^2 \equiv 7 \pmod{83}$ (3) $x^2 \equiv 43 \pmod{109}$

7. 解同余式

(1) $x^2 \equiv 24 \pmod{125}$ (2) $x^2 \equiv 18 \pmod{343}$ (3) $x^2 \equiv 13 \pmod{243}$

8. 解同余式

(1) $x^2 \equiv 57 \pmod{512}$ (2) $x^2 \equiv 41 \pmod{1\,024}$ (3) $x^2 \equiv 17 \pmod{16\,384}$

9. 解同余式

(1) $x^2 \equiv 19 \pmod{90}$ (2) $x^2 \equiv 98 \pmod{343}$ (3) $x^2 \equiv 81 \pmod{729}$

(4) $x^2 \equiv 2\,500 \pmod{3\,125}$ (5) $x^2 \equiv 27 \pmod{243}$

(6) $x^2 \equiv 192 \pmod{512}$

10. 解同余式

(1) $x^2 \equiv 34 \pmod{495}$ (2) $x^2 \equiv 48 \pmod{416}$

11. 解同余式

(1) $8x^2 + 15x - 6 \equiv 0 \pmod{56}$ (2) $12x^2 - 11x - 1 \equiv 0 \pmod{30}$

12. 解同余式

(1) $x^2 + 18x - 18 \equiv 0 \pmod{342}$ (2) $x^2 + x + 4 \equiv 0 \pmod{32}$

13. 解同余式

$x^2 + 8x - 20 \equiv 0 \pmod{45}$

14. 证明:3 是所有形如 $4^n + 1$ 的素数模的平方非剩余。

15. 证明:3 是所有大于 3 的默森尼素数(即形如 $2^q - 1$ 的素数)模的平方非剩余。

16. 证明:(1) 如果 $p \equiv 7 \pmod 8$ 是素数,$q = 4n + 3$ 也是素数,则 $2^q \equiv 1 \pmod p$;

(2) $23 \mid 2^{11} - 1, 47 \mid 2^{23} - 1, 503 \mid 2^{251} - 1$;

(3) 求出 $2^{83} - 1$ 的一个因子。

17. 证明:(1) 如果 p 和 $q = 10p + 3$ 均为奇素数,则 $\left(\frac{p}{q}\right) = \left(\frac{3}{p}\right)$;

(2) 如果 p 和 $q=10p+1$ 均为奇素数,则$\left(\frac{p}{q}\right)=\left(\frac{-1}{p}\right)$。

18. 证明:(1) 如果 $p\equiv 3(\bmod 4)$,且 a 是模p 的平方剩余,则 $p-a$ 就是模 p 的平方非剩余;

(2) $p\equiv 1(\bmod 4)$ 有什么相应于(1) 的结论?

19. 如果 $p>3$ 是一个素数,证明:p 整除它的所有平方剩余之和。

20. (1) 设 $p\geqslant 5$ 是一个素数。如果 $p\equiv 1$ 或 $7(\bmod 12)$,则 -3 是模 p 的平方剩余,如果 $p\equiv 5$ 或 $11(\bmod 12)$,则 -3 是模 p 的平方非剩余;

(2) 设 p 为奇素数,$p\neq 3$,且 $p\nmid a$。又设 $x^3\equiv a(\bmod p)$ 有一个解 r,则

$$(x-r)(x^2+rx+r^2)\equiv 0(\bmod p)$$

证明:当且仅当且 $p\equiv 1$ 或 $7(\bmod 12)$ 时,$x^2+rx+r^2\equiv 0(\bmod p)$ 才具有两个不同于 r 的解;

(3) 如果 $p\geqslant 5$ 是一个素数,则当 $p\equiv 5$ 或 $11(\bmod 12)$ 时,模 p 的不同的非零三次剩余的个数为 $p-1$,当且 $p\equiv 1$ 或 $7(\bmod 12)$ 时,模 p 的不同的非零三次剩余的个数为$\frac{p-1}{3}$。

21. 设 p 为奇素数,计算

$$\left(\frac{1\cdot 2}{p}\right)\left(\frac{2\cdot 3}{p}\right)+\cdots+\left(\frac{(p-2)\cdot(p-1)}{p}\right)$$

3.11 原根和指数

在前面几节中,我们看到在有些问题中,如果对给定的模 m 和整数 a,发现一个整数 n 使得$a^n=1(\bmod m)$,问题就会解决。那么对什么样的整数 a 和m 才会存在具有这种性质的整数 n 呢?答案是:

引理 3.11.1 给定模 m 和整数a,存在正整数 n 使得$a^n=1(\bmod m)$ 的充分必要条件是$(a,m)=1$。换句话说,如果$(a,m)=1$,那么不可能存在一个整数 n 使得$a^n=1(\bmod m)$。当存在这种整数时,必然存在着一个最小的正整数 γ 使得 $a^\gamma\equiv 1(\bmod m)$。

证明 如果$(a,m)=1$,那么从欧拉定理知道,如果$(a,m)=1$,那么 $a^{\varphi(m)}\equiv 1(\bmod m)$,因此所说的整数 n 是存在的。

反过来,如果存在整数 n 使得$a^n\equiv 1(\bmod m)$,那么 $a^{n-1}\cdot a-qm=1$,因此$(a,m)=1$。

定义 3.11.1 设 a,m 都是正整数,$(a,m)=1$,那么使得 $a^\gamma\equiv 1(\bmod m)$ 成立的最小的正整数 γ,称为是 a 对模m 的指数或阶,记为 $\delta_m(a)$。

如果 a 对于模 m 的阶恰等于 $\varphi(m)$，则称 a 是 m 的一个原根。

例如，对模 7，我们有

a	a^2	a^3	a^4	a^5	a^6
1	1	1	1	1	1
2	4	1	2	4	1
3	2	6	4	5	1
4	2	1	4	2	1
5	4	6	2	3	1
6	1	6	1	6	1

因此 3 和 5 的指数为 6，2 和 4 的指数为 3，6 的指数为 2，1 的指数为 1。

取定一个模 m，一个整数的指数并不是可以什么整数都取到的。而是要受到一定的限制，另外并不是每个整数都有原根，例如考虑模 8，小于 8 而与 8 互素的整数为 1，3，5，7，即全体奇数。由此可知 $\varphi(8)=4$。如果 x 是偶数，那么 $x=2k$，因此 $x^4=16k^4\equiv 0 \pmod 8$，即所有的偶数都不可能是模 8 的原根。如果 x 是奇数，那么易证 $x^2\equiv 1 \pmod 8$，因此所有的奇数也不可能是模 8 的原根。这就说明模 8 没有原根。

为了解为什么会有这样的现象，首先需要研究指数有什么性质。为此我们又先要引进剩余系的概念。

在同余式一节中，我们已经知道，给定了一个模 m 后，可以把所有的整数按模 m 分成一些同余类，所谓同余类就是把所有在模 m 下同余的整数所组成的集合分成一类，那么不同的同余类是互不相交的，而全体整数就可以表示成为这些同余类的并。

由同余类的定义可知，取定了模 m 后，共可形成 m 个同余类，这些同余类中的数分别与 $0,1,2,\cdots,m-1$ 同余。

现在从这 m 个同余类的每个类中任意选取一个整数作为代表组成一个集合 K，那么集合 K 具有性质：K 中的元素两两不同余，并且 K 是具有这种性质的最大集合，换句话说，如果向 K 中添加一个任意整数，则 K 中必有两个整数互相同余。由此给出以下定义

定义 3.11.2 设 m 是一个正整数，如果整数的集合 K 具有性质：

(1) K 中的元素两两对模 m 不同余；

(2) K 是具有这种性质的最大集合。

则称 K 是模 m 的一个完全剩余系。

容易证明以下定理：

定理 3.11.1 整数的集合 K 构成模 m 的完全剩余系的充分必要条件是：

(1) K 由 m 个元素组成；

（2）K 中的元素两两不同余。

易证完全剩余系有以下性质：

定理 3.11.2 设 K 是模 m 的一个完全剩余系，则 K 中的元素在对模 m 同余的意义下与集合 $K_0=\{0,1,2,\cdots,m-1\}$ 构成 1—1 对应；

当 m 是偶数时，K 与集合 $-\frac{m}{2},\cdots,-1,0,1,\cdots,\frac{m}{2}-1$ 或者集合 $-\frac{m}{2}+1,\cdots,-1,0,1,\cdots,\frac{m}{2}$ 也构成 1—1 对应；

当 m 是奇数时，K 与集合 $-\frac{m-1}{2},\cdots,-1,0,1,\cdots,\frac{m-1}{2}$ 也构成 1—1 对应。

定义 3.11.3 集合 $K_0=\{0,1,2,\cdots,m-1\}$ 称为模 m 的最小非负完全剩余系，当 m 是偶数时，集合 $-\frac{m}{2},\cdots,-1,0,1,\frac{m}{2}-1$ 或者集合 $-\frac{m}{2}+1,\cdots,-1,0,1,\cdots,\frac{m}{2}$ 称为模 m 的绝对最小完全剩余系，当 m 是奇数时，集合 $-\frac{m-1}{2},\cdots,-1,0,1,\cdots,\frac{m-1}{2}$ 称为模 m 的绝对最小完全剩余系。

现在我们再讨论完全剩余系中与模互素的整数。

定义 3.11.4 从模 m 的完全剩余系中取出所有与 m 互素的整数组成的集合称为模 m 的简化剩余系。

容易证明以下定理：

定理 3.11.3 整数的集合 K 构成模 m 的简化剩余系的充分必要条件是：

（1）K 由 $\varphi(m)$ 个元素组成；

（2）K 中的元素都与 m 互素；

（3）K 中的元素两两互素。

定理 3.11.4 模 m 的任何两个简化剩余系在对模 m 同余的对应下都是 1—1 对应的。

定理 3.11.5 指数有以下性质：

（1）如果 $(a,m)=1,a\equiv b(\bmod m)$，则 $\delta_m(a)=\delta_m(b)$；

（2）如果 $a^n\equiv 1(\bmod m)$，则 $\delta_m(a)\mid n$，或 $n\equiv 0(\bmod \delta_m(a))$，特别，一定有 $\delta_m(a)\mid\varphi(m)$；

（3）如果 $(a,m)=1,a^k\equiv a^h(\bmod m)$，则 $k\equiv h(\bmod \delta_m(a))$；

（4）设 $(a,m)=1$，那么 $1,a^1,\cdots,a^{\delta_m(a)-1}$ 这 $\delta_m(a)$ 对模 m 两两不同余，特别设 g 是 m 的一个原根，则 $1,g,\cdots,g^{\varphi(m)-1}$ 这 $\varphi(m)$ 个数除以 m 所得的余数，恰是小于 m 且与 m 互素的 $\varphi(m)$ 个正整数的一个排列，即它们构成 m 的一个简化剩余系；反之，如果存在一个 g 使得 $1,g,\cdots,g^{\varphi(m)-1}$ 这 $\varphi(m)$ 个数构成 m 的

一个简化剩余系，则 g 就是 m 的一个原根；

(5) 设 b 是 a 对模 m 的逆，即 $ba \equiv 1(\bmod m)$，则 $\delta_m(b) = \delta_m(a)$；

(6) 设 $(a,m) = 1$，k 是非负整数，则 $\delta_m(a^k) = \dfrac{S_m(a)}{(\delta_m(a),k)}$；

此外，在模 m 的简化剩余系中，至少有 $\varphi(\delta_m(a))$ 个数对模 m 的指数等于 $\delta_m(a)$；

(7) $\delta_m(ab) = \delta_m(a)\delta_m(b)$ 的充分必要条件是 $(\delta_m(a),\delta_m(b)) = 1$；一般有如果 $m_1,m_2,\cdots,m_k$ 两两互素，$m = m_1m_1\cdots m_k$，则

$$\delta_m(a) = [\delta_{m_1}(a),\delta_{m_2}(a),\cdots,\delta_{m_k}(a)]$$

(8) 如果 $n \mid m$，则 $\delta_n(a) \mid \delta_m(a)$；

(9) 如果 $(m_1,m_2) = 1$，则 $\delta_{m_1m_2}(a) = [\delta_{m_1}(a),\delta_{m_2}(a)]$；

(10) 设 $(m_1,m_2) = 1$，则对任意的 a_1,a_2，必存在一个 a 使得

$$\delta_{m_1m_2}(a) = [\delta_{m_1}(a_1),\delta_{m_2}(a_2)]$$

一般来说，并不成立 $\delta_m(ab) = [\delta_m(a),\delta_m(b)]$，例如，通过直接计算可以验证

$$\delta_{10}(3\cdot 3) = 2 \neq [\delta_{10}(3),\delta_{10}(3)] = 4$$

$$\delta_{10}(3\cdot 7) = 1 \neq [\delta_{10}(3),\delta_{10}(7)] = 4$$

但是我们有

(11) 对任意的 a,b，一定存在 c，使得

$$\delta_m(c) = [\delta_m(a),\delta_m(b)]$$

证明 (1) 易证(略)。

(2) 设 a 对模 m 的指数为 γ，$n = q\gamma + r, 0 \leqslant r < \gamma$，则根据指数的定义和 n 的性质就有 $a^n \equiv a^{q\gamma+r} \equiv a^{q\gamma}a^r \equiv (a^\gamma)^q a^\gamma (\bmod m)$，因此 $a^r \equiv 1(\bmod m)$。这说明 r 必须等于零，否则 r 将是比 γ 更小的满足关系式 $a^n \equiv 1(\bmod m)$ 的正整数，这与 γ 的最小性相矛盾。这就证明了引理。

由上面已证的性质和费马定理显然立刻得出 $\delta_m(a) \mid \varphi(m)$。

前面提到过取定一个模 m，一个整数的指数并不是可以什么整数都取到的，而是要受到一定的限制，就是指这条性质。

(3) 不失一般性，不妨设 $k \geqslant h$，于是由 $a^k \equiv a^h(\bmod m)$ 得出 $a^{k-h}a^h \equiv a^h(\bmod m)$，再由 $(a,m) = 1$ 和同余式的性质知可把 a^h 约去，于是得到 $a^{k-h} \equiv 1(\bmod m)$。那样，由已证的性质(2) 就得到 $\delta_m(a) \mid (k-h)$ 或者 $k \equiv h(\bmod \delta_m(a))$。

(4) 假如有某两个指标 $k,h, 0 \leqslant k \leqslant \delta_m(a) - 1, 0 \leqslant h \leqslant \delta_m(a) - 1$ 使得 $a^k \equiv a^h(\bmod m)$。不失一般性，不妨设 $k \geqslant h$，那么由(3) 中的证明知 $a^{k-h} \equiv$

$1 \pmod m$，且

$$\delta_m(a) \mid (k-h) < \delta_m(a)$$

这是一个矛盾，所得的矛盾就证明了 $a^0, a^1, \cdots, a^{\delta_m(a)-1}$ 这 $\delta_m(a)$ 个数对模 m 两两不同余。

现在设 g 是 m 的一个原根，则由于 $(g,m)=1$，所以首先得知 g 的各次幂都与 m 互素。并且与上面一样可以证明 $1, g, \cdots, g^{\varphi(m)-1}$ 这 $\varphi(m)-1$ 个数对模 m 两两不同余。因此 $1, g, \cdots, g^{\varphi(m)-1}$ 这 $\varphi(m)$ 个数除以 m 所得的余数，恰是小于 m 且与 m 互素的个正整数的 $\varphi(m)$ 个排列；反过来，如果存在 g 使得 $1, g, \cdots, g^{\varphi(m)-1}$ 这 $\varphi(m)-1$ 个数构成 m 的简化剩余系，则按照原根的定义，g 就是模 m 的原根。

例如，2 是 9 的一个原根，小于 9 而与 9 互素的正整数为 1,2,4,5,7,8，故 $\varphi(9)=6$，而 2 的各次乘幂为

$$2, 2^2, 2^3, 2^4, 2^5, 2^6$$

它们除以 9 所得的余数为 2,4,8,7,5,1，恰为 1,2,4,5,7,8 的一个排列。

(5) 设 $\gamma = \delta_m(a)$，则 $a^\gamma \equiv 1 \pmod m$，$a^1, \cdots, a^{\gamma-1}$ 都不同余于 1 且两两不同余。由 $ba \equiv 1 \pmod m$ 得 $b^i a^i \equiv 1 \pmod m$，$b^i \equiv a^{\gamma-i} \pmod m$，$i=0,1,\cdots,\gamma-1$，由此知道 $b^\gamma \equiv 1 \pmod m$ 且 $1, b^1, \cdots, b^{\gamma-1}$ 都两两不同余，故 $\delta_m(b) = \gamma = \delta_m(a)$。

(6) 设 $\delta = \delta_m(a)$，$\delta' = \dfrac{\delta}{(\delta,k)}$，$\delta^* = \delta_m(a^k)$，则由定义知

$$a^{k\delta^*} \equiv (a^k)^{\delta^*} \equiv 1 \pmod m,\ a^{k\delta'} \equiv a^{\frac{k\delta}{(\delta,k)}} \equiv (a^\delta)^{\frac{k}{(\delta,k)}} \equiv 1 \pmod m$$

因此根据性质(2)立即得出 $\delta \mid k\delta^*$，$\delta^* \mid \delta'$，因而

$$\delta' = \frac{\delta}{(\delta,k)} \Big| \frac{k}{(\delta,k)}\delta^*$$

故

$$\delta' \mid \delta^*$$

但是前面已证又有 $\delta^* \mid \delta'$，由此就得出 $\delta^* = \delta'$，这就是

$$\delta_m(a^k) = \frac{\delta_m(a)}{(\delta_m(a),k)}$$

为证此性质的另一部分，注意如果 $(\delta_m(a),k)=1$，那么由已证明的公式知 a^k 的指数为 $\delta_m(a)$，故至少有 $\varphi(\delta_m(a))$ 个 a^k 的指数为 $\delta_m(a)$。由于 $(a,m)=1$，故 $(a^k,m)=1$。因此这 $\varphi(\delta_m(a))$ 个 a^k 都是属于模 m 的简化剩余类中的元素。这就说明模 m 的简化剩余系中至少有 $\varphi(\delta_m(a))$ 个元素的指数为 $\delta_m(a)$。

(7) 设 $\delta_1 = \delta_m(a)$，$\delta_2 = \delta_m(b)$，$\delta = \delta_m(ab)$，$\lambda = [\delta_m(a), \delta_m(b)]$。

充分性：设 $(\delta_1, \delta_2) = 1$。则我们有

$$1 \equiv (ab)^{\delta} \equiv (ab)^{\delta\delta_2} \equiv a^{\delta_2\delta} (\bmod m)$$

故 $\delta_1 \mid \delta\delta_2$，由于$(\delta_1,\delta_2) = 1$，从而又得出 $\delta_1 \mid \delta$，同理可证 $\delta_2 \mid \delta$，再由$(\delta_1,\delta_2) = 1$ 得出 $\delta_1\delta_2 \mid \delta$。

另一方面，又有$(ab)^{\delta_1\delta_2} \equiv (a^{\delta_1})^{\delta_2}(b^{\delta_2})^{\delta_1} \equiv 1(\bmod m)$，所以又有 $\delta \mid \delta_1\delta_2$。

合并以上两方面的论述就得出 $\delta = \delta_1\delta_2$。这就证明了充分性。

必要性：设 $\delta = \delta_1\delta_2$。则我们有

$$(ab)^{\lambda} \equiv (a^{\delta_1})^{\frac{\lambda}{\delta_1}}(b^{\delta_2})^{\frac{\lambda}{\delta_2}} \equiv 1(\bmod m)$$

故 $\delta \mid \lambda$。另一方面显然有 $\delta \mid \delta_1\delta_2$，因此 $\lambda < \delta$。这就得出 $\lambda = \delta$。再由 $\delta = \lambda(\delta_1,\delta_2)$ 就得出。

(8) 由 $n \mid m$，及 $\delta_m(a)$ 的定义就得出 $a^{\delta_m(a)} \equiv 1(\bmod m) \equiv 1(\bmod n)$，再由性质(2) 就得出 $\delta_n(a) \mid \delta_m(a)$。

(9) 由性质(8) 得出 $\delta^* \mid \delta_{m_1m_2}(a)$，其中 $\delta^* = [\delta_{m_1}(a),\delta_{m_2}(a)]$。另一方面显然有 $a^{\delta^*} \equiv 1(\bmod m_1)$ 及 $a^{\delta^*} \equiv 1(\bmod m_2)$，再由$(m_1,m_2) = 1$ 就得出 $a^{\delta^*} \equiv 1(\bmod m_1m_2)$，因而 $\delta_{m_1m_2}(a) \mid \delta^*$，因此

$$\delta_{m_1m_2}(a) = \delta^* = [\delta_{m_1}(a),\delta_{m_2}(a)]$$

(10) 考虑同余式方程组

$$x \equiv a_1(\bmod m_1), x \equiv a_2(\bmod m_2)$$

由于$(m_1,m_2) = 1$，故由孙子定理知，这个同余式方程组有唯一解

$$x \equiv a(\bmod m_1m_2)$$

由同余式方程组解的定义和性质(1) 即得 $\delta_{m_1}(a) = \delta_{m_1}(a_1)$，$\delta_{m_2}(a) = \delta_{m_2}(a_2)$，由此及性质(10) 即得

$$\delta_{m_1m_2}(a) = [\delta_{m_1}(a_1),\delta_{m_2}(a_2)]$$

(11) 设 $\delta_1 = \delta_m(a)$，$\delta_2 = \delta_m(b)$，$\lambda = [\delta_1,\delta_2]$。我们首先证明可把 δ_1,δ_2 分解成为以下形式：$\delta_1 = \tau_1\lambda_1$，$\delta_2 = \tau_2\lambda_2$，使得$(\lambda_1,\lambda_2) = 1$，$\lambda_1\lambda_2 = \lambda$。分成以下三种情况加以证明：

(i) $(\delta_1,\delta_2) = 1$。这时 $\lambda = [\delta_1,\delta_2] = \delta_1\delta_2$，只要取 $\lambda_1 = \delta_1$，$\lambda_2 = \delta_2$ 即可。

(ii) $(\delta_1,\delta_2) = \delta_1$ 或$(\delta_1,\delta_2) = \delta_2$。由于这两种情况是对称的，故为确定起见，不妨设$(\delta_1,\delta_2) = \delta_1$。这时 $\lambda = [\delta_1,\delta_2] = \delta_2$，只要取 $\lambda_1 = 1$，$\lambda_2 = \delta_2$ 即可。

(iii) $(\delta_1,\delta_2) > 1$。再设 $\delta_1 = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$，$\delta_2 = p_1^{\beta_1}p_2^{\beta_2}\cdots p_k^{\beta_k}$ 分别是δ_1,δ_2 的素因子分解式。$I_1 = \{i \mid 1 \leqslant i \leqslant k, \alpha_i \geqslant \beta_i\}$，$I_2 = \{i \mid 1 \leqslant i \leqslant k, \alpha_i < \beta_i\}$。由于$(\delta_1,\delta_2) > 1$，因此集合 I_1,I_2 都不是空集，而它们的交集是空集。取 $\lambda_1 = \prod_{i\in I_1} p_i^{\alpha_i}$，$\lambda_2 = \prod_{i\in I_2} p_i^{\beta_i}$，则由集合 I_1,I_2 的交集是空集和 $\lambda = [\lambda_1,\lambda_2] = \prod_{i=1}^{k} p_i^{\max(\alpha_i,\beta_i)}$

易证$(\lambda_1,\lambda_2) = 1, \lambda_1\lambda_2 = \lambda$。

这就证明了所说的分解。

由性质(6)得出

$$\delta_m(a^{\tau_1}) = \frac{\delta_m(a)}{(\delta_m(a),\tau_1)} = \frac{\delta_1}{(\delta_1,\tau_1)} = \frac{\tau_1\lambda_1}{(\tau_1\lambda_1,\tau_1)} = \frac{\tau_1\lambda_1}{\tau_1} = \lambda_1$$

同理可得 $\delta_m(b^{\tau_2}) = \lambda_2$。再由$(\lambda_1,\lambda_2) = 1$和性质(7)就得出

$$\delta_m(a^{\tau_1}b^{\tau_2}) = \delta_m(a^{\tau_1})\delta_m(b^{\tau_2}) = \lambda_1\lambda_2 = \lambda = [\delta_m(a),\delta_m(b)]$$

这就说明,我们可取 $c = a^{\tau_1}b^{\tau_2}$。

应用上面的定理,我们可以得出下面这个有实用意义的定理:

定理 3.11.6 设 p 和 q 都是奇素数,且 $q \mid (a^p - 1)$,则或者 $q \mid (a-1)$,或者 $q = 2kp + 1$,其中 k 是一个整数。

证明 由于 $q \mid (a^p - 1)$,因此 $a^p \equiv 1 \pmod q$。故由定理 3.11.1 知 a 的阶 γ 必须是素数 p 的因子,因此 $\gamma = 1$ 或者 $\gamma = p$。如果 $\gamma = 1$,则 $a^1 \equiv a \equiv 1 \pmod q$,因此 $q \mid (a-1)$。如果 $\gamma = p$,则 $\gamma \mid \varphi(q)$,但是 $\gamma = p, \varphi(q) = q - 1$,所以 $p \mid (q-1)$,即存在整数 s 使得 $q - 1 = sp$,但是由于 p, q 都是奇素数,所以 $s = 2k$。

下面我们给出几个和 2 有关的原根和指数的结果。

定理 3.11.7 设 a 是一个大于 1 的奇数,那么

(1) 如果 $a^{2^k} \not\equiv 1 \pmod m$,则对任何 $1 \leqslant i \leqslant k$,都有 $a^{2^i} \not\equiv 1 \pmod m$;

(2) 对 $n \geqslant 2$, $2^{2^{n-1}} \equiv 0 \pmod{2^n}$;

(3) 对 $n \geqslant 3$, $a^{2^{n-2}} \equiv 0 \pmod{2^n}$;

(4) $\delta_{2^n}(a) \mid a^{n-2}$。

证明 (1) 设 $u_k = a^{2^k}$,则对任何 $1 \leqslant i \leqslant k$ 成立 $(u_i)^{2^{k-i}} = u_k$。因此由 $u_i \equiv 1 \pmod m$ 就得出 $u_k \equiv 1 \pmod m$。换句话说如果 $a^{2^k} \not\equiv 1 \pmod m$,则对任何 $1 \leqslant i \leqslant k$,都有 $a^{2^i} \not\equiv 1 \pmod m$。

(2) 对 n 实行数学归纳法。

当 $n = 2$ 时, $2^{2^{2-1}} \equiv 0 \pmod{2^2}$,因此对 $n = 2$,公式 $2^{2^{n-1}} \equiv 0 \pmod{2^n}$ 成立。

假设对所有大于等于 2 小于等于 n 的整数都成立公式 $2^{2^{n-1}} \equiv 0 \pmod{2^n}$,那么 $2^n \mid 2^{2^{n-1}}$,因此 $2^{2^{n-1}} \geqslant 2^n$, $2^{n-1} \geqslant n$,由此得出 $2^{(n+1)-1} = 2^n \geqslant 2n \geqslant n+1$,故 $2^{n+1} \mid 2^{2^n}$,因此对自然数 $n+1$,公式 $2^{2^{n-1}} \equiv 0 \pmod{2^n}$ 仍然成立。故由数学归纳法就证明了对一切大于等于 2 的整数,都成立公式 $2^{2^{n-1}} \equiv 0 \pmod{2^n}$。

(3) 对 n 实行数学归纳法。

当 $n=3$ 时,$2^n=8$,a 是奇数,因此 $a^2\equiv 1(\bmod 8)$,因此公式 $a^{2^{n-2}}\equiv 1(\bmod 2^n)$ 对 $n=3$ 是成立的。

假设对所有大于等于 3 小于等于 n 的整数都成立公式 $a^{2^{n-2}}\equiv 1(\bmod 2^n)$,那么就有

$$a^{2^{n-2}}=2^nq+1$$

把上式的两边都平方就得到

$$a^{2^{n-1}}=(2^nq+1)^2=2^{2n}q^2+2^{n+1}q+1=2^{n+1}(2^{n-1}q+1)q+1$$

或者

$$a^{2^{n-1}}\equiv 1(\bmod 2^{n+1})$$

即对自然数 $n+1$,公式 $a^{2^{n-2}}\equiv 1(\bmod 2^n)$ 仍然成立。所以由数学归纳法就证明了此式对任意 $n\geqslant 3$ 都成立。

(4) 由(3) 和定理 3.11.5 性质(2) 就得出(3)。

由这个定理立刻得出当 $n\geqslant 3$ 时,模 2^n 不存在原根。

从上面所说的结果可以得出模 m 有原根的限制条件,由这些限制条件可以得出:

定理 3.11.8 模 m 存在原根的必要条件是 $m=1,2,4,p^a,2p^a$.

证明 假设 m 存在原根,即存在整数 a,$(a,m)=1$ 和正整数 n 使得 $a^n\equiv 1(\bmod m)$,从而存在一个使这个式子成立的最小正整数 $\delta_m(a)$,而且 $\delta_m(a)=\varphi(m)$。

首先上面已证当 $n\geqslant 3$ 时,模 2^n 不存在原根。因此如果 m 具有形式 2^n,那么 m 只能等于 1,2,4。

其次假设 m 具有形式 $m=2^ak$,$k=p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}$,其中 $p_1,p_2,\cdots,p_k$ 都是奇素数。我们证明必有 $a\leqslant 1$。假设不然,则可设 $a>1$。由于$(2,k)=1$,所以一方面由定理 3.11.5 性质(7) 的证明可知

$$\delta_m(a)\mid[\delta_{2^a}(a),\delta_k(a)]$$

再由定理 3.11.5 性质(2) 可知 $\delta_m(a)\mid[\delta_{2^a(a)},\delta_k(a)]\mid[\varphi(2^a),\varphi(k)]$。而由欧拉函数的计算公式,我们有

$$\varphi(k)=p_1^{a_1-1}p_2^{a_2-1}\cdots p_k^{a_k-1}(p_1-1)(p_2-1)\cdots(p_k-1)$$

注意由于 $p_1,p_2\cdots,p_k$ 都是奇素数,所以 $p_1-1,p_2-1,\cdots,p_k-1$ 都是偶数,因而 $\varphi(k)$ 是偶数。故由于 $a>1$,因此

$$\delta_m(a)\leqslant[\varphi(2^a),\varphi(k)]\leqslant\frac{\varphi(2^a)\varphi(k)}{(\varphi(2^a),\varphi(k))}\leqslant\frac{\varphi(2^a)\varphi(k)}{(2^{a-1},\varphi(k)}\leqslant$$

$$\frac{\varphi(m)}{2\left(2^{a-2},\frac{\varphi(k)}{2}\right)}\leqslant\frac{1}{2}\varphi(m)<\varphi(m)$$

这说明 m 不可能有原根，这就得出必须 $\alpha \leqslant 1$。因此这时 m 只能具有形式

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

或

$$m = 2 p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

其中，$p_1, p_2, \cdots, p_k$ 都是奇素数。

最后我们证明不管 m 是否含有因子 2，它都不可能含有两个以上的奇素数因子。假设不然，则可设 $m = p^{\alpha} q^{\beta} k$，其中 p, q 都是奇素数，k 是与 p, q 都互素的整数。那么 $p - 1, q - 1$ 都是偶数，因此

$$\begin{aligned}\delta_m(a) &\leqslant [\varphi(p^{\alpha}), \varphi(q^{\beta}), \varphi(k)] \leqslant [[\varphi(p^{\alpha}), \varphi(q^{\beta})], \varphi(k)] \leqslant \\ &\left[\frac{\varphi(p^{\alpha})\varphi(q^{\beta})}{(\varphi(p^{\alpha}), \varphi(q^{\beta}))}, \varphi(k)\right] \leqslant \\ &\left[\frac{\varphi(p^{\alpha})\varphi(q^{\beta})}{p^{\alpha-1}(p-1), q^{\beta-1}(q-1))}, \varphi(k)\right] \leqslant \\ &\left[\frac{\varphi(p^{\alpha})\varphi(q^{\beta})}{2\left(\frac{p^{\alpha-1}(p-1)}{2}, \frac{q^{\beta-1}(q-1)}{2}\right)}\right], \varphi(k)] \leqslant \\ &\frac{1}{2}\varphi(p^{\alpha})\varphi(q^{\beta})\varphi(k) \leqslant \frac{1}{2}\varphi(m) < \varphi(m)\end{aligned}$$

故这时 m 也不可能有原根。从而 m 只可能具有形式 $1, 2, 4, p^{\alpha}$ 或者 $2p^{\alpha}$。

那么是不是具有这种形式的模一定具有原根呢？答案是肯定的。我们首先证明：

定理 3.11.9 设 p 是素数，则

(1) 模 p 必存在原根。

(2) 对 $p - 1$ 的每一个因子 d，在模 p 的简化剩余系中恰有 $\varphi(d)$ 个数对模 p 的指数为 d。

证明 设 $1, 2, \cdots, p - 1$ 对模 p 的指数分别为 $\delta_p(1), \delta_p(2), \cdots, \delta_p(p - 1)$。那么由定理 3.11.5 性质(11) 可知，一定存在一个整数 g 使得

$$\delta_p(g) = [\delta_p(1), \delta_p(2), \cdots, \delta_p(p - 1)] = \lambda$$

显然 $\lambda = \delta_p(g) \mid \varphi(p) = p - 1$，以及 $\delta_p(i) \mid [\delta_p(1), \delta_p(2), \cdots, \delta_p(p - 1)] = \lambda$，因此 $\lambda \leqslant p - 1$ 并且同余式方程 $x^{\lambda} \equiv 1 \pmod p$ 或者 $x^{\lambda} - 1 \equiv 0 \pmod p$ 有 $p - 1$ 个解 $x \equiv 1, 2, \cdots, p - 1 \pmod p$，但是由同余式方程的理论知对素数模来说，任何一个同余式方程的解数不可能超过它的次数(见定理 3.9.12)。因此又有 $p - 1 \leqslant \lambda$，联合前面已证明的不等式 $\lambda \leqslant p - 1$ 就得出

$$\delta_p(g) = \lambda = p - 1 = \varphi(p)$$

这就说明 g 就是一个原根。

现在来证明定理的后半部。设 g 是模 p 的一个原根，则由定理 3.11.5 性质(4) 知 $g^0, g^1, \cdots, g^{\varphi(p)-1}$ 这 $\varphi(p) = p - 1$ 个数构成模 p 的一个简化剩余系，现

在的问题是求出这些数中指数等于 d 的数的个数。

由于 d 是一个指数,因此 d 必须整除 $\varphi(p)=p-1$,故可设 $p-1=dr$。我们的目的是找出 $g^0,g^1,\cdots,g^{\varphi(p)-1}$ 中所有指数等于 d 的元素。既然这种元素的指数是 d,所以它们的 d 次方必须同余于 1。现在我们就来看看 $g^0,g^1,\cdots,g^{\varphi(p)-1}$ 中哪些元素的 d 次方可以同余于 1。设元素 g^i 的 d 次方同余于 1,即 $g^{di}\equiv 1(\mathrm{mod}\ p)$。那么由于其中同余 1 的唯一元素是 g^0,以后随着指数的增加,它们循环出现,因此 di 必须是 $\varphi(p)=p-1$ 的倍数,也就是 g^i 的指数 i 必须满足关系式

$$di=k(p-1)=kdr,i=kr$$

所以我们得出所有指数等于 d 的元素的方次数必须是 r 的倍数。

但是具有这种特性的元素中并不是所有的元素的指数都等于 d,而是有的元素的指数可能小于 d。所以我们还必须找出元素 g^{kr} 的指数真正等于 d 的特性来。我们指出这种特性是:

如果 g^{kr} 的指数等于 d,那么必须 $(k,d)=1$。假设不然而有 $(k,d)=h>1$,那么必有 $k=hk_1,d=hd_1,d_1<d$,因此 $kd_1=k_1d$。由此得出

$$(g^{kr})^{d_1}=g^{rkd_1}=g^{rk_1d}=(g^{rd})^{k_1}=(g^{\varphi(p)})^{k_1}\equiv 1(\mathrm{mod}\ p)$$

故 g^{kr} 的指数比小于或等于 $d_1<d$,不可能是 d。这就证明了如果 g^{kr} 的指数等于 d,那么必须 $(k,d)=1$。

现在设 $(k,d)=1$,那么由定理 3.11.5 性质(6),可知

$$\delta_p(g^{kr})=\frac{\delta_p(g)}{(\delta_p(g),kr)}=\frac{\varphi(p)}{(\varphi(p),kr)}=$$

$$\frac{p-1}{(p-1,kr)}=\frac{dr}{(dr,kr)}=\frac{dr}{r(d,k)}=d$$

这就证明了如果 $(k,d)=1$,那么 g^{kr} 的指数就等于 d。因此 g^{kr} 的指数等于 d 的充分必要条件就是 $(k,d)=1$,由此就得出使得 $(k,d)=1$ 的 k 的个数和使得 g^{kr} 的指数等于 d 的 k 的个数同样多,这也就是说在模 p 的简化剩余系中,指数等于 d 的元素的个数就等于 $\varphi(d)$。

为了由此定理得出下面的结果,我们首先证明以下引理。

引理 3.11.2 设 g 是 p 的原根,那么

(1) $g^{p-1}=1+pT_0$;

(2) $(g+pt)^{p-1}=1+pu$,从而对每一个整数,都唯一地确定了一个对应的整数 u,使得 $u=u(t)$ 是 t 的函数值为整数的函数;

(3) $u(t)\equiv T_0-g^{p-2}t(\mathrm{mod}\ p)$;

(4) 存在 t_0 使得 $p\nmid u_0=u(t_0)$。

证明 (1) 由于 g 是 p 的原根,故由欧拉定理知 $g^{\varphi(p)}=g^{p-1}\equiv 1(\mathrm{mod}\ p)$,

因此就得出

$$g^{p-1} = 1 + pT$$

(2) 由

$$(g + pt)^{p-1} \equiv g^{p-1} \pmod p$$

即得出
$$(g + pt)^{p-1} = 1 + pu$$

这也就是说 $u = \dfrac{(g + pt)^{p-1} - 1}{p}$ 确定了 t 的函数值为整数的函数。

(3)
$$\begin{aligned}(g + pt)^{p-1} &= g^{p-1} + C_{p-1}^{1} g^{p-2} pt + p^2 T^* \\ &= g^{p-1} + (p - 1) g^{p-2} pt + p^2 T^* \\ &= 1 + pT_0 - g^{p-2} pt + g^{p-2} p^2 t + p^2 T^* \\ &= 1 + pT_0 - g^{p-2} pt + p^2 T \\ &= 1 + p(T_0 - g^{p-2} t + pT)\end{aligned}$$

其中 T^* 和 T 都是 t 的整系数多项式,因此

$$u = T_0 - g^{p-2} t + pT \equiv T_0 - g^{p-2} t \pmod p$$

(4) 由于 g 是 p 的原根,所以 $(g, p) = 1$,从而 $(g^{p-2}, p) = 1$。因此一次同余式方程

$$g^{p-2} x \equiv T_0 \pmod p$$

有唯一解 x_0。设 $t_0 \not\equiv x_0 \pmod p$,则

$$u_0 = u(t_0) \not\equiv g^{p-2} t_0 - T_0 \pmod p$$

因此 $p \nmid u_0$。

引理 3.11.3 设 $\alpha > 1$,那么

(1) 如果 $a^n \equiv 1 \pmod{p^\alpha}$,则 $a^{pn} \equiv 1 \pmod{p^{\alpha+1}}$;

(2) 如果 $a^n = 1 + p^\alpha u_0$, $a^{pn} = 1 + p^{\alpha+1} u$,则 $u_1 \equiv u_0 \pmod p$。

证明 (1) 由 $a^n \equiv 1 \pmod{p^\alpha}$ 得出 $g^n = 1 + p^\alpha u_0$,因此

$$\begin{aligned}a^{pn} &= (a^n)^p = (1 + p^\alpha u_0)^p = 1 + C_p^1 p^\alpha u_0 + p^{2\alpha} K \\ &= 1 + p^{\alpha+1} u_0 + p^{2\alpha} K \\ &= 1 + p^{\alpha+1}(u_0 + p^{\alpha-1} K)\end{aligned}$$

其中,K 是整数,并且最后一步用到了 $2\alpha - (\alpha + 1) = \alpha - 1 > 0$,这就得出

$$a^{pn} \equiv 1 \pmod{p^{\alpha+1}}$$

(2) 由(1)中的证明知 $u_1 = u_0 + p^{\alpha-1} K$,因此 $u_1 \equiv u_0 \pmod p$。

现在我们可以证明:

定理 3.11.10 设 g 是 p 的原根,t_0 是引理 3.11.2(4) 中所保证存在的具有性质 $p \nmid u_0$ 的整数,则对任意正整数 α,$g + pt_0$ 是模 p^α 的原根。

证明 由引理 3.11.2 和引理 3.11.3 知

$$(g+pt_0)^{p-1}=1+pu_0$$
$$(g+pt_0)^{p(p-1)}=(1+pu_0)^p=1+p^2u_1$$
$$(g+pt_0)^{p^2(p-1)}=(1+p^2u_1)^p=1+p^3u_2$$
$$\vdots$$
$$(g+pt_0)^{p^n(p-1)}=(1+p^nu_{n-1})^p=1+p^{n+1}u_n$$

而且

$$u_0\equiv u_1\equiv\cdots\equiv u_n\equiv\cdots(\bmod p)$$

现在设 $g+pt_0$ 对模 p^α 的指数为 δ，则

$$(g+pt_0)^\delta\equiv 1(\bmod p^\alpha)$$

由此得出

$$(g+pt_0)^\delta\equiv 1(\bmod p)$$

所以 $a=g+pt_0\equiv g(\bmod p)$ 是模 p 的原根，因此

$$a^0,a^1,\cdots,a^{p-1}$$

中唯一同余于 1 的元素是 a^0，且随着 a 的方次数的增加，每隔 $p-1$ 次循环出现。这就得出 δ 必须是 $p-1$ 的倍数，即 $(p-1)\mid\delta$。

另一方面由 δ 的定义知

$$\delta\mid\varphi(p^\alpha)=p^{\alpha-1}(p-1)$$

这说明 δ 必须有如下形式

$$\delta=p^{r-1}(p-1),1\leqslant r\leqslant\alpha$$

利用上式又得出

$$1+p^ru_{r-1}=(g+pt_0)^{p^{r-1}(p-1)}\equiv 1(\bmod p^\alpha)$$

因此

$$p^ru_{r-1}\equiv 0(\bmod p^\alpha)$$

注意 $u_{r-1}\equiv u_{r-2}\cdots\equiv u_0(\bmod p)$，$p\nmid u_0$，因此 $p\nmid u_{r-1}$。这就得出 $p^\alpha\mid p^r$，故

$$\alpha\leqslant r\leqslant\alpha,r=\alpha$$

这也就是说

$$\delta=p^{r-1}(p-1)=p^{\alpha-1}(p-1)=\varphi(p^\alpha)$$

因此 $g+pt_0$ 是模 p^α 的原根。

为了给出 $2p^\alpha$ 的原根，我们先证明下面的引理：

引理3.11.4 设 x 是一个奇数，则 $x^n\equiv 1(\bmod p^\alpha)$ 成立的充分必要条件是

$$x^n\equiv 1(\bmod 2p^\alpha)$$

证明 如果 $x^n\equiv 1(\bmod 2p^\alpha)$，则由于 $p^\alpha\mid 2p^\alpha$，故 $x^n\equiv 1(\bmod p^\alpha)$；反过来，如果 $x^n\equiv 1(\bmod p^\alpha)$，则由于 x 是奇数，所以 $x\equiv 1(\bmod 2)$，$x^m\equiv 1(\bmod 2)$。由于 $(2,p^\alpha)=1$，故 $x^n\equiv 1(\bmod 2p^\alpha)$。

定理 3.11.11 设 $\alpha \geqslant 1$，g 是模 p^α 的一个原根，则 g 和 $g+p^\alpha$ 二者之中的奇数就是模 $2p^\alpha$ 的原根。

证明 设 g 是奇数，则由 g 是模 p^α 的原根的定义就得出

$$g^{\varphi(p^\alpha)} \equiv 1(\bmod p^\alpha), g^r \not\equiv 1(\bmod p^\alpha), 0 < r < \varphi(p^\alpha)$$

再由上面的引理就得出

$$g^{\varphi(p^\alpha)} \equiv 1(\bmod 2p^\alpha), g^r \not\equiv 1(\bmod 2p^\alpha), 0 < r < \varphi(p^\alpha)$$

这就说明 g 是模 $2p^\alpha$ 的原根。

同理可证 $g+p^\alpha$ 是奇数的情况。

由于当 $m=1,2,4$ 时原根分别为 $1,1,-1$，因此由定理 3.11.9，定理 3.11.10 和定理 3.11.11 就得出

定理 3.11.12 设 p 是奇素数模，$\alpha \geqslant 1$，则 m 存在原根的充分必要条件是

$$m = 1,2,4,p^\alpha,2p^\alpha$$

由上面的定理和定理 3.11.5(4) 就得出：

定理 3.11.13 设 p 是奇素数模，$\alpha \geqslant 1$，则当且仅当

$$m = 1,2,4,p^\alpha,2p^\alpha$$

时，模 m 的简化剩余系能表为 $g^0, g^1, \cdots, g^{\varphi(m)-1}$ 的形式，其中 g 为某一个整数。

虽然以上定理给出了原根存在的充分必要条件，并且也实际给出了原根存在时的求法，但是要具体对一个模确定出它的原根却并不容易。

例如，我们可利用以上定理确定 100 以内以 2 为原根的素数只有 3,5,11,13,19,29,37,53,59,61,67,83，但是至今尚无法得出一个定理能说出哪些素数以 2 为原根，甚至无法确定以 2 为原根的素数是否有无限多个，因此下面的这个定理就显得很有趣。

定理 3.11.14 设 p 和 $4p+1$ 都是奇素数，则 2 是 $4p+1$ 的原根。

证明 设 $q=4p+1$，由于 $\varphi(q)=4p$。故 2 的指数只可能是 $1,2,4,p,2p$ 或 $4p$。我们证明前 5 种情况都不可能出现。

由于 p 是奇数，故

$$4p = 4(2k+1) = 8k+4(4(\bmod 8)$$

$$q = 4p+1 \equiv 5(\bmod 8)$$

此外根据欧拉判据和勒让德符号的意义还有

$$2^{2p} \equiv 2^{\frac{q-1}{2}} \equiv \left(\frac{2}{q}\right)(\bmod q)$$

而由定理 3.10.40 知

$$\left(\frac{2}{q}\right) = (-1)^{\frac{q^2-1}{8}} = -1$$

故

$$2^{2p} \equiv -1(\bmod q)$$

这说明2的指数不可能是$2p$的因子$1,2,p$以及$2p$。2的指数也不可能是4，否则由$2^4\equiv 1(\mathrm{mod}\ q)$得出$q\mid 15$，因此由$q$是$4p+1$形式的素数又得出$q=5$，但是由于$p\geqslant 3$，所以这又和$q$是$4p+1$形式的奇素数矛盾，因此$q\geqslant 13$，与$q=5$矛盾。

因此只能有$\delta_q(2)=4p=\varphi(q)$，这就是说2是$q$的原根。

利用此定理和素数表中的$q-1$行，我们可知，如果此行中的分解式具有形式2^2p，则2就是q的原根。由此立刻得出149，173，293，317，389等都是以2为原根的素数。

在高中的数学课中，我们知道对数是一个很有用的概念，它可以把乘法运算化为加法运算，在理论上也起着不可缺少的作用。如果m是一个具有原根的整数，那么我们也可以定义一个类似于对数的概念。

定义 3.11.5 设$(a,m)=1$，如果$a\equiv g^{\gamma}(\mathrm{mod}\ m)$，$\gamma\geqslant 0$，则$\gamma$就称为模$m$的以$g$为底的指标，记为$\gamma=\mathrm{ind}_g a$（或$\gamma=\mathrm{ind}\ a$）。

由定理3.11.5(4)知，如果g是模m的原根，则$g^0,g^1,\cdots,g^{\varphi(m)-1}$就是模的简化剩余系。因此对每一个与$m$互素的$a$，在$0,1,2,\cdots,\varphi(m)-1$之中必存在一个唯一的指标$\gamma'=\mathrm{ind}_g a$使得$a\equiv g^{\gamma'}(\mathrm{mod}\ m)$。知道了$\gamma'$，根据定理3.11.5(1)就可求出$a$的所有指标，这些指标就是$\gamma'$的在模$\varphi(m)$下的同余类中的非负整数，即$a$的任何指标都要满足关系式

$$\gamma\equiv r'(\mathrm{mod}\ \varphi(m)),\gamma\geqslant 0$$

指标具有下面的类似于对数的性质：

定理 3.11.15 设$a_1,a_2,\cdots,a_n$是与m互素的n整数，则

$$\mathrm{ind}(a_1a_2\cdots a_n)\equiv\mathrm{ind}\ a_1+\mathrm{ind}\ a_2+\cdots+\mathrm{ind}\ a_n(\mathrm{mod}\ \varphi(m))$$

特别
$$\mathrm{ind}\ a^n\equiv n\,\mathrm{ind}\ a(\mathrm{mod}\ \varphi(m))$$

证明 由指标的定义即得出

$$a_1\equiv g^{\mathrm{ind}\ a_1}(\mathrm{mod}\ m),a_2\equiv g^{\mathrm{ind}\ a_2}(\mathrm{mod}\ m),\cdots,a_n\equiv g^{\mathrm{ind}\ a_n}(\mathrm{mod}\ m)$$

把它们连乘起来就得到

$$a_1a_2\cdots a_n\equiv g^{\mathrm{ind}\ a_1+\mathrm{ind}\ a_2+\cdots+\mathrm{ind}\ a_n}(\mathrm{mod}\ m)$$

因此$\mathrm{ind}\ a_1+\mathrm{ind}\ a_2+\cdots+\mathrm{ind}\ a_n$就是$a_1a_2\cdots a_n$一个指标，故

$$\mathrm{ind}(a_1a_2\cdots a_n)\equiv\mathrm{ind}\ a_1+\mathrm{ind}\ a_2+\cdots+\mathrm{ind}\ a_n(\mathrm{mod}\ \varphi(m))$$

在上式中令$a_1=a_2=\cdots=a_n=a$就得到$\mathrm{ind}\ a^n\equiv n\,\mathrm{ind}\ a(\mathrm{mod}\ \varphi(m))$。

正像利用对数表和反对数表可以求n次方根一样，我们也可以编出指标表和反指标表来解同余式

$$x^n\equiv a(\mathrm{mod}\ m),(a,m)=1\text{（当然首先需要模 }m\text{ 存在原根）}$$

例如，对$p=41$，由上面所讲的内容可以确定6是模41的原根，于是以6做底，通过实际计算可以得出下列各式

$$6^0 \equiv 1, 6^8 \equiv 10, 6^{16} \equiv 18, 6^{24} \equiv 16, 6^{32} \equiv 32$$
$$6^1 \equiv 6, 6^9 \equiv 19, 6^{17} \equiv 26, 6^{25} \equiv 14, 6^{33} \equiv 17$$
$$6^2 \equiv 36, 6^{10} \equiv 32, 6^{18} \equiv 33, 6^{26} \equiv 2, 6^{34} \equiv 20$$
$$6^3 \equiv 11, 6^{11} \equiv 28, 6^{19} \equiv 34, 6^{27} \equiv 12, 6^{35} \equiv 38$$
$$6^4 \equiv 25, 6^{12} \equiv 4, 6^{20} \equiv 40, 6^{28} \equiv 31, 6^{36} \equiv 23$$
$$6^5 \equiv 27, 6^{13} \equiv 24, 6^{21} \equiv 35, 6^{29} \equiv 22, 6^{37} \equiv 15$$
$$6^6 \equiv 39, 6^{14} \equiv 21, 6^{22} \equiv 5, 6^{30} \equiv 9, 6^{38} \equiv 8$$
$$6^7 \equiv 29, 6^{15} \equiv 3, 6^{23} \equiv 30, 6^{31} \equiv 13, 6^{39} \equiv 7$$

利用上面的计算结果，就可编制出模 41 的以 6 为底的指标表和反指标表。

其中指标表是用来从真数查指标的，而反指标表是用来从指标查真数的。

表 3.11.1　模 41 的以 6 为底的指标表

	0	1	2	3	4	5	6	7	8	9
0		0	26	15	12	22	1	39	38	30
1	8	3	27	31	25	37	24	33	16	9
2	34	14	29	36	13	4	17	5	11	7
3	23	28	10	18	19	21	2	32	35	6
4	20									

表 3.11.2　模 41 的以 6 为底的反指标表

	0	1	2	3	4	5	6	7	8	9
0	1	6	36	11	25	27	39	29	10	19
1	32	28	4	24	21	3	18	26	33	34
2	40	35	5	30	16	14	2	12	31	22
3	9	31	37	17	20	38	23	15	8	7

这些表中的最左边的纵行中的数字表示已知数字的十位数，而最上边的横行中的数字表示已知数字的个位数。例如要查模 41 的以 6 为底的真数 30 的指标是多少，你可以在指标表中最左边的纵行中先找到数字 3，然后在这一行中对着最上边一行中的数字 0 所在的列和这一行的交叉处找到数字 23，这就表示 30 的指标是 23，即 ind 30 = 23。同理可以查出 15 的指标是 37，即 ind 15 = 37。

反过来在反指标表中，用同样的方法，可以查出指标是 33 的真数为 17，即 33 = ind 17；指标是 15 的真数为 3，即 15 = ind 3。

下面我们利用指标理论来研究二项式同余式方程

$$x^n \equiv a \pmod{m}$$

类似于平方剩余的概念，我们引进所谓 n 次剩余的概念：

定义 3.11.6 设 m 是正整数，如果同余式方程 $x^n \equiv a(\bmod m)$，则称 a 是模 m 的 n 次剩余，反之则称 a 是模 m 的 n 次非剩余。

定理 3.11.16 设 $m \geqslant 2, (a, m) = 1, (n, \varphi(m)) = d$，且模 m 存在原根 g，则

(1) 同余式方程 $x^n \equiv a(\bmod m)$ 有解（即 a 是模 m 的 n 次剩余）的充分必要条件是

$$d \mid \mathrm{ind}_g a$$

且在有解时，解数是 d。

(2) 在模 m 的简化剩余系中，n 次剩余的个数是 $\frac{\varphi(m)}{d}$。

证明 (1) 我们证明同余式方程 $x^n \equiv a(\bmod m)$ 和同余式方程 $nx \equiv \mathrm{ind}_g a(\bmod \varphi(m))$ 同时有解或者同时无解。

设同余式方程 $x^n \equiv a(\bmod m)$ 有解，且 $x \equiv c(\bmod m)$ 是 $x^n \equiv a(\bmod m)$ 的解，则由 $(a, m) = 1$ 知 $(c, m) = 1$。故由 g 是原根的性质知，必存在正整数 k 使得 $c = g^k(\bmod m)$（定理 3.11.13）。因而有

$$g^{kn} = c^n \equiv a(\bmod m)$$

故由定理 3.11.5 性质(2) 和 g 是原根得出

$$kn \equiv \mathrm{ind}_g a(\bmod \varphi(m))$$

这说明同余式方程 $nx \equiv \mathrm{ind}_g a(\bmod \varphi(m))$ 有解。

反之，如果同余式方程 $nx \equiv \mathrm{ind}_g a(\bmod \varphi(m))$ 有解 $x \equiv k(\bmod \varphi(m))$，那么

$$nk \equiv n\frac{\mathrm{ind}_g a}{d} \equiv \frac{n}{d}\mathrm{ind}_g(a) = h\,\mathrm{ind}_g(a) = \mathrm{ind}_g(a)(\bmod \varphi(m))$$

因而

$$g^{kn} \equiv a(\bmod m)$$

这就说明 $c = g^k$ 是同余式方程 $x^n \equiv a(\bmod m)$ 的解。因而同余式方程 $x^n \equiv a(\bmod m)$ 有解。

此外，从定理 3.11.5 性质(3) 知如果 $c_1 \equiv g^{k_1}(\bmod m)$，$c_2 \equiv g^{k_2}(\bmod m)$，那么 $c_1 \equiv c_2(\bmod m)$ 的充分必要条件是 $k_1 \equiv k_2(\bmod \varphi(m))$（注意当 g 是原根时 $\delta_m(g) = \varphi(m)$），因此同余式方程 $x^n \equiv a(\bmod m)$ 的解数和同余式方程 $nx \equiv \mathrm{ind}_g a(\bmod \varphi(m))$ 的解数相同。

由一次同余式方程的理论知同余式方程 $nx \equiv \mathrm{ind}_g a(\bmod \varphi(m))$ 有解的充分必要条件是 $(n, \varphi(m)) = d \mid \mathrm{ind}_g a$，并且有解时的解数是 $(n, \varphi(m)) = d \mid \mathrm{ind}_g a$（定理 3.9.4），这就证明了定理。

在解普通的代数方程 $x^n = a, a \geqslant 0$ 时，我们知道可以用两边取对数的方法见其化为一个对数方程 $n\log_c x = \log_c a$，然后通过查对数表和反对数表就可

把这个方程解出来。一般我们取 $c=10$ 或 $c=e$。所以我们很自然地想到，对二项同余式方程有没有类似的结果。回答是有的。这就是

定理 3.11.17 设 $m\geqslant 2,(a,m)=1$，且模 m 存在原根 g，则同余式方程

$$x^n\equiv a \pmod m$$

与同余式方程

$$n\,\mathrm{ind}_g x\equiv \mathrm{ind}_g a \pmod{\varphi(m)}$$

同解。

证明 设同余式方程 $x^n\equiv a\pmod m$ 有解 $x\equiv c\pmod m$，那么 $c^n\equiv a\pmod m$。因而由指标的性质（定理 3.11.15）即得 $n\,\mathrm{ind}_g x\equiv \mathrm{ind}_g a\pmod{\varphi(m)}$。反之，如果有整数 c 适合同余式方程 $n\,\mathrm{ind}_g x\equiv \mathrm{ind}_g a\pmod{\varphi(m)}$，则由定理 3.11.15 和 g 是原根的性质（定理 3.11.5 性质(1)，(4)）就可知成立同余式 $x^n\equiv a\pmod m$。这就证明了定理。

由此得到：

定理 3.11.18 设 $m\geqslant 2,(a,m)=1,(n,\varphi(m))=d$，且模 m 存在原根 g，则 a 是模 m 的 n 次剩余的充分必要条件是 $a^{\frac{\varphi(m)}{d}}\equiv 1\pmod m$。

证明 由定理 3.11.16 知 a 是模 m 的 n 次剩余的充分必要条件是

$$d\mid \mathrm{ind}_g a$$

或者

$$\mathrm{ind}_g a\equiv 0\pmod d$$

由同余式的性质（定理 3.6.4(11)）和 $d\mid\varphi(m)$ 即知这个条件就是

$$\frac{\varphi(m)}{d}\mathrm{ind}_g a\equiv 0\pmod{\varphi(m)}$$

也就是

$$a^{\frac{\varphi(m)}{d}}\equiv 1\pmod m$$

任给 $(a,m)=1$，且设模 m 有原根 g，则对于 a 来说，我们已经定义了两个概念，一个是 a 的指数 $\delta_m(a)$，它是指满足同余式 $a^n\equiv 1\pmod m$ 的最小正整数 n，另一个称为 a 的指标 $\mathrm{ind}_g a$，它是指满足关系式 $a=g^\gamma\pmod m$ 的正整数 γ。现在我们要问这两个数之间有什么关系，如何用这些数来给出 a 是否是原根的判据，对这两个问题，我们有：

定理 3.11.19 设 $m\geqslant 2,(a,m)=1$，且模 m 存在原根 g，则

$$\delta_m(a)=\frac{\varphi(m)}{(\mathrm{ind}_g a,\varphi(m))}$$

且 a 是模 m 的原根的充分必要条件是 $(\mathrm{ind}_g a,\varphi(m))=1$。

证明 设 $\gamma=\mathrm{ind}_g a$，则 $a=g^\gamma\pmod m$。由定理 3.11.5 性质(6) 即得

$$\delta_m(a)=\delta_m(g^\gamma)=\frac{\delta_m(g)}{(\gamma,\delta_m(g))}=\frac{\varphi(m)}{(\mathrm{ind}_g a,\varphi(m))}$$

如果 a 是模 m 的原根，则 $\delta_m(a)=\varphi(m)$，因此 $(\mathrm{ind}_g a,\varphi(m)=1)$，反之如果 $(\mathrm{ind}_g a,\varphi(m))=1$，则 $\delta_m(a)=\varphi(m)$，因此 a 是模 m 的原根。

此外，我们还要注意，从这个定理的证明看出，不论以模 m 的哪一个原根为底，定理的结论都是不变的。也就是说上述定理的结论与我们所取的原根无关。

最后我们给出一个定理 3.11.9 的推广（请注意下面的定理和定理 3.11.9 的条件的区别）。

定理 3.11.20 在模 m 的简化剩余系中，指数是 d 的整数的个数是 $\varphi(d)$，特别原根的个数是 $\varphi(\varphi(m))$。

证明 设在模 m 的简化剩余系中有 T 个整数的指数是 d，则由定理 3.11.19 知

$$d=\frac{\varphi(m)}{(\mathrm{ind}_g a,\varphi(m))}$$

故

$$(\mathrm{ind}_g a,\varphi(m))=\frac{\varphi(m)}{d}$$

因此 T 就等于模 m 的简化剩余系中满足条件 $(\mathrm{ind}_g a,\varphi(m))=\frac{\varphi(m)}{d}$ 的整数的个数。由原根的定义知，当 $\mathrm{ind}_g x$ 通过 $0,1,\cdots,\varphi(m)-1$ 时（也就是 g 的方次数通过 $0,1,\cdots,\varphi(m)-1$ 时），$g^{\mathrm{ind}_g a}=x$ 就通过 m 的简化剩余系，因此反过来说就是当 x 通过 m 的简化剩余系时，$\mathrm{ind}_g x$ 就通过 $\varphi(m)$ 的最小完全剩余系。这也就是说，T 就是满足关系式

$$(y,\varphi(m))=\frac{\varphi(m)}{d},0\leqslant y<\varphi(m)$$

的整数的个数，令 $y=\frac{\varphi(m)}{d}z$，则 T 就是满足关系式

$$\left(\frac{\varphi(m)}{d}z,\varphi(m)\right)=\frac{\varphi(m)}{d},0\leqslant\frac{\varphi(m)}{d}z<\varphi(m)$$

的整数的个数，把上述各式都除以 $\frac{\varphi(m)}{d}$ 就得到 T 就是满足关系式

$$(z,d)=1,0<z<d$$

的整数的个数。因此得出 $T=\varphi(d)$。特别由于原根的指数是 $\varphi(m)$，因此原根的个数就等于 $\varphi(\varphi(m))$。

虽然我们在原则上已经解决了在模 m 有原根的情况下如何去求出模 m 的原根的问题，但是下面这个定理，在实际计算模 m 的原根时，有时还是比较方便的。

定理 3.11.21 设 $m>1$，$\varphi(m)$ 的所有的不同的素因数是 $p_1,p_2,\cdots,p_k$，$(g,m)=1$，则 g 是模 m 的原根的充分必要条件是

$$g^{\frac{\varphi(m)}{p_i}} \not\equiv 1(\bmod\ m), i = 1,2,\cdots,k$$

证明 (1) 如果 g 是模 m 的原根，则 g 对模 m 的指数是 $\varphi(m)$。但是由于

$$0 < \frac{\varphi(m)}{p_i} < \varphi(m), i = 1,2,\cdots,k$$

因此

$$g^{\frac{\varphi(m)}{p_i}} \not\equiv 1(\bmod\ m), i = 1,2,\cdots,k$$

(否则和 g 是模 m 的原根的假设相矛盾)。

(2) 假设 $g^{\frac{\varphi(m)}{p_i}} \not\equiv 1(\bmod\ m), i = 1,2,\cdots,k$，$g$ 对模 m 的指数是 δ。如果 $\delta < \varphi(m)$，则由定理3.11.5可知 $\delta \mid \varphi(m)$。因此 $\frac{\varphi(m)}{\delta}$ 是一个大于1的整数 k，k 当然有素因子，而且 k 的素因子显然只能是 $\varphi(m)$ 的素因子(因为 k 本身是 $\varphi(m)$ 的因子)，也就是所必有 $\varphi(m)$ 的某个素因子 $p_i \mid \frac{\varphi(m)}{\delta} = k$，于是 $\frac{\varphi(m)}{\delta} = p_i q$ 或者 $\frac{\varphi(m)}{p_i} = q\delta$，因此

$$g^{\frac{\varphi(m)}{p_i}} \equiv g^{q\delta} \equiv (g^{\delta})^q \equiv 1(\bmod\ m)$$

这和假设 $g^{\frac{\varphi(m)}{p_i}} \not\equiv 1(\bmod\ m), i = 1,2,\cdots,k$ 矛盾。所得的矛盾表明必须 $\delta = \varphi(m)$，故 g 是模 m 的原根。

例 3.11.1 判断同余式方程 $x^8 \equiv 23(\bmod 41)$ 是否有解。

解 $n = 8, \varphi(41) = 40, d = (8,40) = 8$。又通过查指标表知道 ind 23 = 36(注意结果和底无关，因此我们不必写出底来)。由于 $8 = d \nmid 36 = \text{ind}\ a$，因此方程 $x^8 \equiv 23(\bmod 41)$ 无解。

例 3.11.2 解同余式方程 $x^{12} \equiv 37(\bmod 41)$。

解 $d = (12,40) = 4$，又通过查指标表知道 ind 37 = 32，由于 $d \mid \text{ind}\ 37$，故由定理3.11.16知方程 $x^{12} \equiv 37(\bmod 41)$ 有 $d = 4$ 个解。

为了求出这4个解，你需要解同余式 $nx \equiv \text{ind}_g a(\bmod\ \varphi(m))$ 或者 $12x \equiv 32(\bmod 40)$，由同余式的性质(定理3.6.4(11))，它等价于 $3x \equiv 8(\bmod 10)$，这个模不大，因此这个方程不难解，而且用观察法容易看出 $3 \cdot 3 \equiv 9 \equiv -1(\bmod 10)$，因此用3去乘以方程 $3x \equiv 8(\bmod 10)$ 的两边就得到 $-x \equiv 24(\bmod 10) \equiv -6(\bmod 10)$，因此 $x \equiv 6(\bmod 10)$。回到原来的模40，即得到模40下的4个解为 $k \equiv 6,16,26,36(\bmod 40)$，因而方程 $x^{12} \equiv 37(\bmod 41)$ 的4个解为 $x \equiv 6^6, 6^{16}, 6^{26}, 6^{36}(\bmod 41)$，也就是 $x \equiv 39,18,2,23(\bmod 41)$。

例 3.11.3 求对模41的4次剩余的个数。

解 由定理3.11.16知，对模41的4次剩余的个数等于

$$\frac{\varphi(41)}{(4,\varphi(41))}=\frac{40}{(4,40)}=\frac{40}{4}=10$$

而由实际计算可知，在模 41 的最小非负剩余中，模 41 的 4 次剩余（显然只须要计算在模 41 的最小非负剩余中，模 41 的 4 次剩余，由于当数超过 41 时，再产生的 4 次剩余将和模 41 的最小非负剩余中，某个模 41 的 4 次剩余同余）是

$$1,4,10,16,18,23,25,31,37,40$$

恰好也是 10 个，所以定理 3.11.16 的结论和实际计算的结果是吻合的。

例 3.11.4 求在模 41 的简化剩余系中，指数是 10 的元数的个数和原根的个数。

解 根据定理 3.11.20 在模 41 的简化剩余系中，指数是 10 的元素的个数为

$$T=\varphi(10)=4$$

而原根的个数为

$$\varphi(\varphi(41))=\varphi(40)=16$$

而实际上，指数是 10 的元素 a 满足条件 $(\text{ind } a,40)=\frac{40}{10}=4$，它们是

$$a=4,23,25,31$$

恰好是 4 个，与定理 3.11.20 的结论一致。而原根是满足条件

$$(\text{ind } a,40)=1$$

的元素 a，即

$$\text{ind } a=1,3,7,9,11,13,19,21,23,27,29,31,33,37,39$$

$$a=6,11,29,19,28,24,26,34,35,30,12,22,13,17,15,7$$

这些数的个数是 16 也与定理 3.11.20 的结论一致。

例 3.11.5 求出模 41 的最小原根。

证明 $m=41,\varphi(m)=\varphi(41)=40=2^3\cdot 5$，故 $\varphi(41)$ 有两个不同的素因子 $p_1=2$ 和 $p_2=5$。$\frac{\varphi(m)}{p_1}=\frac{40}{2}=20,\frac{\varphi(m)}{p_2}=\frac{40}{5}=8$。故 g 是模 41 的原根的充分必要条件是

$$g^8\not\equiv 1(\text{mod } 41),g^{20}\not\equiv 1(\text{mod } 41),g\nmid 41$$

我们用 $1,2,3,4,\cdots$ 逐一验算得到

$$1^8\equiv 1(\text{mod } 41),2^8\equiv 10(\text{mod } 41),3^8\equiv 1(\text{mod } 41)$$

$$2^{20}\equiv 1(\text{mod } 41)$$

$$4^8\equiv 18(\text{mod } 41),5^8\equiv 18(\text{mod } 41),6^8\equiv 10(\text{mod } 41)$$

$$4^{20}\equiv 1(\text{mod } 41),5^{20}\equiv 18(\text{mod } 41),6^{20}\equiv 40(\text{mod } 41)$$

计算到此停止，而根据定理 3.11.21 我们发现模 41 的最小原根是 6。

现在来谈这一节的最后一个问题，就是对没有原根的模，如何构造它的简

化剩余系。有的读者可能不解，说你怎么老要纠缠这个什么简化剩余系的构造问题呢？其原因就在于他们还没有体会到这个问题的重要。其实只要回忆一下关于原根和指数的一系列结果是怎么得到的，你就会发现，几乎所有的结果都依赖于有原根的模的简化剩余系有很好的构造。

那么有原根的模的简化剩余系的构造到底好在哪呢？为体会这点，我们先看模 m 的完全剩余系的构造，这个构造是非常清楚的，就是任何连续的 $m-1$ 个整数都构成 m 的一个完全剩余系，这里完全剩余系中元素的个数，元素的表达式都很清楚，最简单的表达式就是 $0,1,2,\cdots,m-1$。

但是简化剩余系的构造就不那么清楚了，除了知道它的元素个数 $\varphi(m)$ 是外，把简化剩余系的元素按大小排起来，恐怕你只能写出它的第一个元素 1 和最后一个元素 $m-1$，其他的元素的表达式是什么就写不出来了。

然而如果模 m 有原根 g，它的简化剩余系的构造就令人惊奇地很清楚了，就是

$$g^0,g^1,\cdots,g^{\varphi(m)-1}$$

这 $\varphi(m)$ 个数，这里简化剩余系的个数和表达式都有，注意，上面那些数的方次数可都是连续的，只不过把简化剩余系中元素的大小顺序重新排列了一下，就能得出这样清楚的结构，这恐怕是当初你没有想到的吧。

正因为有原根的模的简化剩余系的构造如此之好，所以人们对没有原根的模就感到格外遗憾了，因为它们的简化剩余系不可能有同样的构造。对不可能的事你当然就无法办到，所以人们就退而求其次，考虑是否能对它们构造出结构尽可能清楚，表达式尽可能简单的简化剩余系的问题了。

我们不准备全面解答这个问题，只想提供一个解决问题的导引和范例。

首先考虑形如 2^n 的模，我们已经知道当 $n\geqslant 3$ 时，它是没有原根的。我们再来复习一下它没有原根的原因。如果一个模 m 有原根 g，g 必须有两个性质，第一个性质是 g 的 $\varphi(m)$ 次方必须同余于 1，这句话几乎是废话，因为对任何一个整数 a，$(a,m)=1$，a 的 $\varphi(m)$ 次方都同余于 1。所以关键是第二个性质，那就是对比 $\varphi(m)$ 小的任何正整数 k，g 的 k 次方都不能同余于 1。我们知道 $\varphi(2^n)=2^{n-1}$，而由定理 3.11.7 我们知道当 $n\geqslant 3$ 时，$2^{2^{n-2}}\equiv(\bmod 2^n)$ 也就是说，使 2^k 同余于 1 的方次数恰比 $\varphi(2^n)=2^{n-1}$ 小了一个数量级，或者说，使 2^k 同余于 1 的方次数提前一个数量级到达了，这样当 $n\geqslant 3$ 时 2^n 就不可能有原根了。

现在我们的问题是，使 2^k 同余于 1 的方次数还能不能更提前？也就是问是否存在比 2^{n-2} 更小的 k，使得对任意 $(a,2)=1$ 都有 $2^k\equiv 1(\bmod 2^n)$。回答是没有了。那也就是说，存在一个数 ξ，使得 $\xi^{2^{n-2}}\equiv 1(\bmod 2^n)$，而且对于任何比 2^{n-2} 更小的正整数 k，2^k 都不同余于 1，有了这两条，这个 ξ 的性质虽然达不到原根

那样好，也已经是尽可能地好了，因为 ξ 的使 2^k 同余于 1 的方次数只比原根小了一个数量级，这样，虽然我们还不能写出 2^n 的全部简化剩余系，但是至少可以写出它的简化剩余系的一半来，这就是 $\xi^0,\xi^1,\cdots,\xi^{2^{n-2}-1}$。

如果能再找出另一半来，那虽然不能得到像原根那样好的简化剩余系来，也已经获得了一个我们想要的结构尽可能清楚，表达式尽可能简单的简化剩余系了。

下面我们就来证明 ξ 的存在性，以及如何用 ξ 来构造 2^n 的简化剩余系。

为此先证明下述引理：

引理 3.11.5 对任意非负整数 m 成立

$$5^{2^m}=1+2^{m+2}+2^{m+3}u_m$$

其中，u_m 是一个非负整数。

证明 利用数学归纳法证明。

当 $m=0$ 时，$5^{2^0}=5^1=1+4+8\cdot 0$；

当 $m=1$ 时，$5^{2^1}=5^2=1+8+16\cdot 1$；

当 $m=2$ 时，$5^{2^2}=5^4=1+16+32\cdot 19$。

因此引理对 $m=0,1,2$ 都成立。

假设对 $m-1$ 引理成立，即设 $5^{2^{m-1}}=1+2^{m+1}+2^{m+2}u_{m-1}$，那么

$$\begin{aligned}5^{2^m}&=(5^{2^{m-1}})^2=(1+2^{m+1}+2^{m+2}u_{m-1})^2\\&=1+2^{m+2}+2^{m+3}(2^{m-1}+u_{m-1}+2^{m+1}u_{m-1}+2^{m+1}u_{m-1}^2)\\&=1+2^{m+2}+2^{m+3}u_m\end{aligned}$$

其中 $u_m=2^{m-1}+u_{m-1}+2^{m+1}u_{m-1}+2^{m+1}u_{m-1}^2$ 是一个非负整数。

因此由数学归纳法就证明了引理。

定理 3.11.22 设 $n\geqslant 3$，则 5 对模 2^n 的指数是 2^{n-2}，并且

$$\pm 5^0,\ \pm 5^1,\cdots,\ \pm 5^{2^{n-2}-1}$$

是模 2^n 的简化剩余系。

证明 由上面的引理显然就得出 $5^{2^{n-1}}\equiv 1(\bmod 2^n)$，而如果 $m<n-2$，那么 5^{2^m} 必定不可能同余于 1，假设不然，设 $5^{2^m}\equiv 1(\bmod 2^n)$，则

$$5^{2^m}=1+2^{m+2}+2^{m+3}u_m=1+2^nq$$

因此
$$2^{m+2}+2^{m+3}u_m=2^nq$$

在上式两边同除以 2^{m+2} 就得到 $1+2u_m=2^{n-m-2}q$，这显然是一个矛盾，所得的矛盾就证明了当 $m<n-2$ 时，不可能成立 $5^{2^m}\equiv(\bmod 2^n)$。

综合以上两点就得出当 $n\geqslant 3$ 时，5 对模 2^n 的指数是 2^{n-2}。由此得出

$$5^0, 5^1, \cdots, 5^{2^{n-2}-1}$$

是两两不同余的，因而 $-5^0, -5^1, \cdots, -5^{2^{n-2}-1}$ 也是两两不同余的。不仅如此任一个 5^s 和任一个 -5^t 对模 2^n 也是不同余的，因为 $5^s \equiv 1 \pmod 4$ 而 $-5^t \equiv -1 \pmod 4$。由上面两行数中的每一个数显然都与 2^n 互素，且共有 $2 \cdot 2^{n-2} = \varphi(2^n)$ 个数，因此 $\pm 5^0, \pm 5^1, \cdots, \pm 5^{2^{n-2}-1}$ 就是模 2^n 的一个简化剩余系。

这样我们就对没有原根的模 2^n 求出了一个简化剩余系，看起来，它的结构和表达式也都是相当清楚和简单的，所以这是一个令人满意的结果。也为求出其他没有原根的模的简化剩余系提供了一个范例，而如何对一个没有原根的模去求出它的一个结构尽可能清楚，表达式尽可能简单的简化剩余系也成了一个进一步研究的课题。有兴趣的读者可以继续深入地去钻研这个问题。

习题 3.11

1. 设 $m = 5,11,12,13,14,15,17,19,20,21,23,36,40,63$。

(1) 如果 m 有原根，求出模 m 的最小完全剩余系中的所有原根以及模 m 的最小正原根；

(2) 如果 m 没有原根，求出模 m 的最小完全剩余系中所有对模 m 的指数为最大的整数。

2. 求 $\delta_{41}(10), \delta_{43}(7), \delta_{55}(2), \delta_{65}(8), \delta_{91}(11), \delta_{69}(4), \delta_{231}(5)$。

3. 设 $m = 2^{\alpha_0} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$，其中 $p_1, p_2, \cdots, p_k$ 是不同的奇素数。

$$\lambda(m) = [2^{c_0}, \varphi(p_1^{\alpha_1}), \varphi(p_2^{\alpha_2}), \cdots, \varphi(p_k^{\alpha_k})]$$

其中

$$c_0 = \begin{cases} 0, \alpha_0 = 0,1 \\ 1, \alpha_0 = 2 \\ \alpha_0 - 2, \alpha_0 \geqslant 3 \end{cases}$$

(1) 证明：当 $(m,n) = 1$ 时，$\lambda(mn) = [\lambda(m), \lambda(n)]$；

(2) 设 d 是给定的正整数，m 是使得 $\lambda(n) = d$ 的最大正整数 n，证明：如果 $\lambda(n) = d$，则 $n \mid m$。

4. 设 $m = 5,11,12,13,14,15,17,19,20,21,,23,36,40,63$。

如果 m 没有原根，求出模 m 的最小完全剩余系中所有对模 m 的指数为最大的整数；把所求出的最大指数和 3 题中的 $\lambda(m)$ 相比较。

5. 证明：3 是 1 459 的最小正原根。

6. 设 $m > 1, (ab, m) = 1, \lambda = (\delta_m(a), \delta_m(b))$.

证明：(1) $\lambda^2 \delta_m((ab)^\lambda) = \delta_m(a)\delta_m(b)$；

(2) $\lambda^2 \delta_m(ab) = (\delta_m(ab), \lambda)\delta_m(a)\delta_m(b)$。

7. 设 $n \geqslant 1, p, q$ 都是奇素数，$q = 2^n p + 1$。又设 a 是模 q 的平方非剩余，且

满足 $a^{2^n} \not\equiv 1 \pmod q$，则 a 是 q 的原根。

8. 证明：(1) $2^{17} - 1 = 131\,071$ 是素数；

(2) $\dfrac{2^{19}+1}{3}$ 是素数。

9. (1) 设 $n > 1$，$p = 2^n + 1$ 是素数，证明：3 是 p 的原根；

(2) 设 $n > 1$，$m = 2^n + 1$，证明：m 是素数的充分必要条件是 $3^{\frac{m-1}{2}} \equiv -1 \pmod m$。

10. 设 $p = 2^{4n} + 1$ 是素数，证明：7 是 p 的原根。

11. 证明：10 是模 17 及模 257（257 是素数）的原根，并由此证明把 $\frac{1}{17}$ 和 $\frac{1}{257}$ 化成循环小数时，循环节的长度必为 16 和 256。

12. 证明：10 是 487 的原根，但不是 487^2 的原根。

13. 对 $p = 11, 13, 17, 19, 31, 37, 53, 71$ 求出 g，使得对所有的 $\alpha \geqslant 1$，它是 p^α，$2p^\alpha$ 的原根。

14. 设 $k \geqslant 1$，p 是素数，证明：

$$1^k + 2^k + \cdots + (p-1)^k \equiv \begin{cases} 0 \pmod p, & (p-1) \nmid k \\ -1 \pmod p, & (p-1) \nmid k \end{cases}$$

15. 利用指标表解以下同余式方程

(1) $3x^6 \equiv 5 \pmod 7$　　(2) $x^{12} \equiv 16 \pmod{17}$

(3) $5x^{11} \equiv -6 \pmod{17}$　　(4) $3x^{14} \equiv 2 \pmod{23}$

(5) $x^{15} \equiv 14 \pmod{41}$　　(6) $7x^7 \equiv 11 \pmod{41}$

(7) $3^x \equiv 2 \pmod{23}$　　(8) $13^x \equiv 5 \pmod{23}$

16. 对哪些 a，同余式方程 $ax^5 \equiv 3 \pmod{19}$ 可解？

17. 对哪些 b，同余式方程 $7x^8 \equiv b \pmod{41}$ 可解？

18. 设 p 是奇素数。证明：同余式方程 $x^4 \equiv -1 \pmod p$ 有解的充分必要条件是 $p \equiv 1 \pmod 8$。由此推出形如 $8m + 1$ 的素数有无穷多个。

19. 解同余式方程

(1) $x^6 \equiv -15 \pmod{64}$　　(2) $x^{12} \equiv 7 \pmod{128}$

(3) $3x^6 \equiv 7 \pmod{2^5 \cdot 31}$　　(4) $5x^4 \equiv 3 \pmod{2^5 \cdot 23 \cdot 19}$

20. 求 53^2 的 26 次剩余。

21. 证明：如果素数 $p \equiv 5 \pmod 8$，则同余式方程 $x^4 \equiv -1 \pmod p$ 无解。

22. 设 p 是素数，证明：同余式方程 $x^8 \equiv 16 \pmod p$ 一定有解。

23. 证明：2 是模 73 的 8 次剩余。

24. 解同余式方程 $(x^2+1)(x+1)x \equiv -1 \pmod{41}$。

25. 设素数 $p \equiv 3 \pmod 4$。证明：a 是模 p 的 4 次剩余的充分必要条件是 $\left(\frac{a}{p}\right) = 1$，即 a 是模 p 的二次剩余。求解同余式方程 $x^4 \equiv 3 \pmod{11}$。

有理数的性质

第四章

4.1 用小数表示有理数

我们对整数已经很熟悉了，而有理数可以说是与整数关系最密切的非整数了。下面我们给出有理数的严格定义。

定义 4.1.1 设 $r=\frac{m}{n}$，$n\neq 0$，其中 m，n 都是整数，则称 r 是一个有理数。

当然如果有人抬杠，说你这不过是同义重复，因为假定一个人只知道整数的含义，你首先就要说明 $\frac{m}{n}$ 是什么意思才能使用这个符号。我说他说的没有错，但是本书就不准备从这么基础的工作讲起了，因为这种工作对不是专门从事数学基础研究的读者来说，实在是有点繁琐乏味。所以我们认为 $\frac{m}{n}$ 的含义就是各位在小学里已经学过的那些解释，并以此为基础讲解。

根据有理数的定义和分数的含义我们可以得出有理数也就是分数的加减乘除四则运算的法则，这些法则读者都是从小学起就很熟悉的了。然而从实用的角度来看，大家也一定早都感觉到按这些法则进行的计算要比对整数进行计算要麻烦得多，所

以在实用的计算中,我们几乎从不使用分数直接进行计算,而首先要把分数化成为小数。下面我们就来详细地研究一下如何用小数来表示一个有理数。

用小数来表示有理数的问题是和进位制紧密联系在一起的,因为在不同的进位制下,小数的表示是不一样的。

首先看把一个数在我们最熟悉的十进制下表示成为小数是什么意思。比如我们要问 120.374 5 是什么意思,可能没有人不知道,但是知道的深浅可能不一样,最普通的答案是 120.374 5 就表示 120 再加上 0.374 5。但是再追问一句,120 又是什么意思?0.374 5 又是什么意思?恐怕有的人就不愿回答了(或者说就是回答不出来了),你要是问急了,他的说法就是 120 就是 120。也就是他认为这个 120 已经无法再进一步解释了。实际上 120 还可以进一步解释为 1 个 100 再加上 2 个 10 再加上 0 个 1,同样 0.374 5 也可以进一步解释为 3 个$\frac{1}{10}$再加上 7 个$\frac{1}{100}$再加上 4 个$\frac{1}{1\,000}$再加上 5 个$\frac{1}{10\,000}$。或者写得更简明一些,我们可以说 120 就是 1 个 10^2 再加上 2 个 10^1 再加上 0 个 10^0,而 0.374 5 就是 3 个$\frac{1}{10}$再加上 7 个$\frac{1}{10^2}$再加上 4 个$\frac{1}{10^3}$再加上 5 个$\frac{1}{10^4}$。

那么这样解释 120.374 5 究竟有什么用处呢?有的人可能会认为纯粹自找麻烦。从表面上看可能如此,但是如果我问你在十进位制下

$$a_na_{n-1}\cdots a_1a_0.a_{-1}a_{-2}\cdots a_{-m}\cdots, 0\leqslant a_i\leqslant 9$$

是什么意思,在 7 进位制下,160406 又是什么意思,那恐怕只有这样解释才说得清楚。例如在十进位制下

$$a_na_{n-1}\cdots a_1a_0.a_{-1}a_{-2}\cdots a_{-m}\cdots = 10^na_n+10^{n-1}a_{n-1}+\cdots+10a_1+a_0+\frac{a_{-1}}{10}+\frac{a_{-2}}{10^2}+\cdots+\frac{a_{-m}}{10^m}+\cdots$$

而在 7 进位制下 $160406=1\cdot 7^5+6\cdot 7^4+0\cdot 7^3+4\cdot 7^2+0\cdot 7+6$。为了更加明确起见,我们通常把上面的式子写成

$$(160406)_7=1\cdot 7^5+6\cdot 7^4+0\cdot 7^3+4\cdot 7^2+0\cdot 7+6=(31\,415)_{10}$$

上面数字外括弧下方的数字表示括弧中的数字是以其为进位制的基。

我们从上面的例子就可知道,要想表示一个数字,必须先确定一个称为基的数字,然后就可以用这个基来表示所有的数字,显然最小的基只能是 2。

说明:在用通常的十进小数表示数时,我们就已知道,有的数(例如$\frac{1}{3}$)只能用无限小数来表示。当我们用无限小数来表示一个数时,通过无穷级数的计算就会发现,一个数字可能有两种表示方法,例如

$$0.999\cdots = \frac{9}{10} + \frac{9}{10^2} + \frac{9}{10^3} + \cdots = \frac{\frac{9}{10}}{1 - \frac{1}{10}} = 1$$

为了避免这种不确定性，我们可以通过约定在这两种表示方法中一律采用哪一种来消除这种不确定性。在一般情况下，如果一个数字既可以表示成为无限小数也可以表示成有限小数，则我们总是把它表示成为有限小数，或者说在用小数表示一个数时，我们采用有限优先原则。在此约定下，每一个数的小数表示就是唯一的。但是有时我们也约定把所有的小数都表示成无限的形式来达到唯一性，到底采用哪种约定可根据我们解决问题时的需要和方便来决定。

下面先给出两个小数比大小的法则。

定理 4.1.1 设在基 b 下

$$\alpha = a_n a_{n-1} \cdots a_0 . a_{-1} a_{-2} \cdots, \beta = c_n c_{n-1} \cdots c_0 . c_{-1} c_{-2} \cdots$$

其中 $0 \leqslant a_i < b, 0 \leqslant c_i < b$，$k$ 是从左向右数时的第一个使得 $a_i \neq c_i$ 的下标。如果 $a_k > c_k$，则 $\alpha > \beta$。

证明 设 $\gamma = a_n b^n + \cdots a_{k+1} b^{k+1}$，则由于 $a_k > c_k$，因此 $a_k - 1 \geqslant c_k$，此外按照我们的约定，$c_{k-1}, c_{k-2}, \cdots$ 不可能都是 $b-1$，而 $c_{k-1}, c_{k-2}, \cdots$ 最大只可能是 $b-1$，因此必存在某一个指标 i 使得 $b - 1 > c_i, j < k$。因此

$$\begin{aligned}\alpha &= \gamma + a_k b^k + a_{k-1} b^{k-1} + \cdots \geqslant \gamma + a_k b^k \\ &\geqslant \gamma + (a_k - 1) b^k + (b-1) b^{k-1} + (b-1) b^{k-2} + \cdots \\ &\geqslant \gamma + c_k b^k + c_{k-1} b^{k-1} + c_{k-2} b^{k-2} + \cdots \geqslant \beta\end{aligned}$$

下面我们证明，可以用任意一个大于 1 的正整数作为基来表示有理数。

定理 4.1.2 对任意的正整数 $b > 1$，每一个有理数 r 都可以以唯一的方式表示成

$$r = a_n b^n + a_{n-1} b^{n-1} + \cdots + a_1 b + a_0 + \frac{a_{-1}}{b} + \frac{a_{-2}}{b^2} + \cdots + \frac{a_{-m}}{b^m} + \cdots$$

的形式，其中 $1 \leqslant a_n < b, 0 \leqslant a_i < b, i < n$。同时对 $i < n$，a_i 不全为 0。即在基 b 下，每一个有理数 r 都可以以唯一的方式表示成 b 进制小数 $r = a_n a_{n-1} \cdots a_2 a_1 a_0 . a_{-1} a_{-2} \cdots a_{-m} \cdots$。

证明 不妨设 $r > 0$。再设

$$\begin{aligned}r &= q_1 b + r^*, 0 \leqslant r^* < b \\ q_1 &= q_2 b + a_1, 0 \leqslant a_1 < b \\ q_2 &= q_3 b + a_2, 0 \leqslant a_2 < b \\ &\vdots\end{aligned}$$

由于 $r > q_1 > q_2 > q_3 > \cdots$，且每个 q_i 都是非负数，因此必存在一个 n 使得

$$q_n = 0 \cdot b + a_n, 0 < a_n < b$$

这样就有

$$\begin{aligned} r &= r^* + q_1 b = r^* + (a_1 + q_2 b) b = r^* + a_1 b + q_2 b^2 \\ &= r^* + a_1 b + (a_2 + q_3 b) b^2 = r^* + a_1 b + a_2 b^2 + q_3 b^3 \\ &= \cdots = r^* + a_1 b + \cdots + a_n b^n \end{aligned}$$

再设

$$\begin{aligned} & r^* = [r^*] + \{r^*\} = a_0 + r_0, 0 \leqslant a_0 \leqslant b, 0 \leqslant r_0 < 1 \\ & br_0 = [br_0] + \{br_0\} = a_{-1} + r_{-1}, 0 \leqslant a_{-1} < b, 0 \leqslant r_{-1} < 1 \\ & br_{-1} = [br_{-1}] + \{br_{-1}\} = a_{-2} + r_{-2}, 0 \leqslant a_{-2} < b, 0 \leqslant r_{-2} < 1 \\ & \vdots \end{aligned}$$

于是

$$r^* = a_0 + r_0 = a_0 + \frac{a_{-1}}{b} + \frac{r_{-1}}{b} = a_0 + \frac{a_{-1}}{b} + \frac{a_{-2}}{b^2} + \frac{r_{-2}}{b^2} = \cdots =$$

$$a_0 + \frac{a_{-1}}{b} + \frac{a_{-2}}{b^2} + \cdots + \frac{a_{-m}}{b^m} + \cdots$$

把 r^* 代入到上面 r 的表示式中，就得到

$$r = a_n b^n + a_{n-1} b^{n-1} + \cdots + a_1 b + a_0 +$$

$$\frac{a_{-1}}{b} + \frac{a_{-2}}{b^2} + \cdots + \frac{a_{-m}}{b^m} + \cdots$$

为证明唯一性，我们假设 r 在基 b 下有两个不同的表示式 α 和 β 如下（如果 α 和 β 的位数不同，我们可以在位数较少的那个数之前补上若干个 0 使它们的位数相同）。

$$\alpha = a_n a_{n-1} \cdots a_0 . a_{-1} a_{-2} \cdots, \beta = c_n c_{n-1} \cdots c_0 . c_{-1} c_{-2} \cdots$$

那么既然 α 和 β 是不同的表示式，因此当我们从左向右数时，必存在一个指标 k 使得 $a_k \neq c_k$，不妨设 $a_k > c_k$，于是根据定理 4.1.1 就得出 $r = \alpha > \beta = r$，这个矛盾就说明了 r 的表示式是唯一的。

把有理数表示成为小数虽然带来了实际计算上的方便，但是也随之产生了另一种遗憾，那就是大部分有理数用小数表示时都是无限小数，而在实际中，我们只能对有限小数进行可操作的计算，因此计算的结果都是近似的。你要想精确，就得舍弃实际计算的方便，回到封闭形式的分数表示上去。这就是宇宙中无处不在、无时不在的矛盾性的一种表现。

有的读者可能会问，是否存在一个基，使得在这个基下，所有的分数都能表示成为有限小数？回答是不可能，因为我们有下面的定理。

定理 4.1.3 设 $r = \frac{p}{q}$，$(p, q) = 1$，b 的素因子是 $p_1, p_2, \cdots, p_k$。则 r 在 b 进

制下是一个有限小数的必要条件 q 的素因子集合是 $\{p_1,p_2,\cdots,p_k\}$ 的子集。

证明 设在 b 进制下，r 是一个有限小数，$r = a_0.a_{-1}a_{-2}\cdots a_{-n}$，其中 $0 \leqslant a_i < b(i > -n)$，$1 \leqslant a_{-n} < b$。于是

$$r = a_0 + \frac{a_{-1}a_{-2}\cdots a_{-n}}{b^n} = \frac{a_0 b^n + a_{-1}a_{-2}\cdots a_{-n}}{b^n} = \frac{p}{q},(p,q) = 1$$

由于 q 是分母和分子约分的结果，故显然 q 的素因子集合只可能是 b 的素因子集合的子集。

由此定理易于得出存在无穷多个有理数，其 b 进制小数表示是无穷小数。而由于 b 的任意性，因此我们就知道，不可能存在一个基，使得在这个基下，所有的分数都能表示成为有限小数。

最常用的基就是我们最熟悉的 10，其他还有 2，这个基在计算机技术中应用得非常广泛，其特点就是运算法则的简单，但是缺点是表示出来的数字非常长，是所有的基中最长的。60 也是一种常用的基，在表示角度、时间时经常采用这种进位制。在天文、航空、航海事业中应用的非常广泛。

为了求出一个十进位数用 b 作基时的表示式，最好采用定理 4.1.2 的证明中所用的格式。例如要将 31415 化成以 8 为基的数，按照定理 4.1.2 的证明中所用的格式，我们可重复地用 8 相除得到

$$31415 = 8 \cdot 3926 + 7$$
$$3926 = 8 \cdot 490 + 6$$
$$490 = 8 \cdot 61 + 2$$
$$61 = 8 \cdot 7 + 5$$
$$7 = 8 \cdot 0 + 7$$

因此

$$31415_{10} = 75267_8$$

注意 75267 正好是上面的除法式子中最后一排余数从下向上写再横排过来所得的数。

反过来，要把 8 进制数 75267 化成 10 进制的数可以用下面的式子计算

$$75267_8 = 7 + 6 \cdot 8 + 2 \cdot 8^2 + 5 \cdot 8^3 + 7 \cdot 8^4 =$$
$$7 + 48 + 128 + 2560 + 28762 =$$
$$31\ 415$$

例 4.1.1

(1) 求出 $2^n - 1$ 能被 7 整除的充分必要条件；

(2) 证明：对任何正整数 n，$2^n + 1$ 不可能被 7 整除。

解 (1) 由于

$$7 = 111_2, 2^n - 1 = \underbrace{11\cdots11_2}_{n个1}$$

因此显然就可看出，当且仅当 2^n-1 的 2 进制表示中的位数 n 是 7 的 2 进制表示中的位数 3 的倍数时，2^n-1 才能被 7 整除，也即 2^n-1 能被 7 整除的充分必要条件是 $n=3k$，其中 k 是一个非负整数。

(2) 由

$$2^1+1\equiv 3 \pmod 7$$
$$2^2+1\equiv 5 \pmod 7$$
$$2^3+1\equiv 2 \pmod 7$$
$$2^4+1\equiv 3 \pmod 7$$

可知，当 $n=1,2,3,\cdots$ 时，2^n+1 被 7 除的余数为 $3,5,2,3,5,2,\cdots$ 循环出现，因此 2^n+1 被 7 除的余数永远不可能为 0，故对任何正整数 n，2^n+1 不可能被 7 整除。

下面我们再利用二进制小数来证明一个关于无限集合势的定理。

定理 4.1.4　设 $a_n=1$ 或 $0(n=1,2,3,\cdots)$，$T=\{(a_1,a_2,\cdots,a_n,\cdots)\}$，这里各个 a_n 的值的取法是互相独立的，那么集合 T 的势就是 c。

证明　T 中有一部分元素从某一位起全是 0，设这种元素所组成的集合为 S。S 中的每一个元素 $(a_1,a_2,\cdots,a_n,\cdots)$ 对应于一个以有限形式表示的二进小数 $0.a_1a_2\cdots a_n$，$a_{n+1}=a_{n+2}=\cdots=0$，这个小数所表示的数或者是 1 或者是 $\frac{m}{2^n}$（就像任何一个有限的十进小数都可写成 $\frac{m}{10^n}$ 的形式一样），因而 S 构成有理数的一个子集，所以 S 是可数集合。按照本节前面的说明，从所有的二进小数构成的集合中除去 S 后（即除去所有用有限形式表示的二进小数后），所有 $(0,1]$ 中的数的二进小数表示就是唯一的了，即映射 $(a_1,a_2,\cdots,a_n,\cdots)\rightarrow 0.a_1a_2\cdots a_n\cdots$ 构成了集合 $T\setminus S$ 和 $(0,1]$ 之间的一个 1—1 对应。这就证明了 $T\setminus S$ 的势是 c，因而 T 的势是 c。

习题 4.1

1. 以下列数为基写出 1 492

(1)2　　(2)3　　(3)7　　(4)9　　(5)11；

2. 计算

(1)3141_5　　(2)3141_6　　(3)3141_7　　(4)3141_9

3. 求出 x

(1)$123_4=x_5$　　(2)$234_5=x_6$　　(3)$123_x=1002_4$

4. 计算（本题中所有的数均以 7 为基）

(1)15 + 24 + 33　　(2)314 + 152 + 265 + 351

(3)42.12　　(4)314.152

5. 将下列各数写成 10 进制分数

(1)$(0.25)_7$　(2)$(0.333\cdots)_7$　(3)$(0.545454\cdots)_7$

6. b 为哪些数时，1111_b 可被 5 整除？

7. (1) 证明：$123_7, 132_7, 312_7, 231_7, 321_7, 213_7$ 都是偶数；

(2) 证明：以 7 为基时，一个整数是偶数的充分必要条件是它的各位数字之和是偶数。

8. (1) 证明：$121_3 = 4^2, 121_4 = 5^2, 121_5 = 6^2$；

(2) 根据(1) 的结果，猜想一个定理，并证明这个定理；

(3) 以 10 为基，计算 169_b 的值($b \geqslant 10$)。

9. 下面两个数中哪个数较大？

$$174 + \frac{7}{13} + \frac{12}{13^2} + \frac{8}{13^3} + \frac{9}{13^4} + \frac{10}{13^5}$$

$$174 + \frac{7}{13} + \frac{11}{13^2} + \frac{12}{13^3} + \frac{11}{13^4} + \frac{12}{13^5}$$

10. 一个企业家答应赠送 100 000 元给一些数学家，然而附加条件是数学家们必须设计一种赠款方案使得：

(1) 每份赠款的价值必须是 2 的方幂；

(2) 每份赠款的价值都不相同。

问这些数学家如何才能得到这笔赠款？

11. 甲乙二人赌博，规则是第一局的赌注是一元(也即每人押一元，谁赢了钱就归谁，或赢者获得两元)，第二局是 2 元，依次类推，每一局的赌注都是前一局的 2 倍。赌了 8 局后，甲赢得 31 元，问甲赢了哪几局？

12. 一个天平的两个盘子上都允许放置砝码，为了称出质量为 1 g，2 g，…，100 g 的试剂，至少需要几个砝码？

13. 证明：$(2^m - 1) \mid (2^n - 1), 0 < m \leqslant n$ 的充分必要条件是 $m \mid n$。

14. 设 $m > 2$，m, n 都是正整数，则 $2^n + 1$ 不可能被 $2^m - 1$ 整除。

15. 设 $f(n)$ 表示 $U_n = (x^2 + x + 1)^n$ 中奇系数的个数，$n = 2^{k_1}n_1 + 2^{k_2}n_2 + \cdots + 2^{k_l}n_l$，其中

$$k_1 < k_2 < \cdots < k_l$$

$$n_1 = 1 + 2 + \cdots + 2^{h_1}, h_1 + k_1 < k_2 - 1$$

$$n_2 = 1 + 2 + \cdots + 2^{h_2}, h_2 + k_2 < k_3 - 1$$

$$\vdots$$

$$n_{l-1} = 1 + 2 + \cdots + 2^{h_{l-1}}, h_{l-1} + k_{l-1} < k_l - 1$$

$$n_l = 1 + 2 + \cdots + 2^{h_l}$$

证明：(1) $f(n) = f(n_1)f(n_2)\cdots f(n_l)$；

(2) $f(1+2+2^2+\cdots+2^k)=2\left[\dfrac{2^{k+2}-1}{3}\right]$。

4.2 有理数的10进小数表示的特性

我们在上一节中已经知道,任何一个有理数都可表示为小数形式,特别是10进小数形式。然而这还不足以揭露出有理数的特性来。在实际计算中,我们会发现有理数化为10进小数时,可能会化为有限小数或循环小数,其中循环小数又分为纯循环小数和混循环小数。本节的目的就是要证明任何一个有理数都必然可化成上述三种形式的小数之一,并给出有理数可化为这几种小数的充分必要条件。

以下的数字和小数均为10进制表示。

定理4.2.1 设有理数 $r=\dfrac{p}{q},(p,q)=1$,则 r 是一个有限小数的充分必要条件是

$$q=2^s5^t,s\geqslant 0,t\geqslant 0$$

证明 (1) 设 $p=qc_0+p_1,0\leqslant p_1<q,q=2^s5^t$,则

$$r=c_0+\frac{p_1}{q},(p_1,q)=1$$

(否则 $(p,q)=(c_0q+p_1,q)=(p_1,q)>1$,与 $(p,q)=1$ 矛盾)

不妨设 $s\geqslant t$,于是

$$r=c_0+\frac{p_1}{q}=c_0+\frac{p_1}{2^s5^t}=c_0+\frac{5^{s-t}p_1}{10^s},0\leqslant 5^{s-t}p_1<10^s$$

这就证明了 r 是一个有限小数。

对 $s\leqslant t$ 的情况同理可证。

(2) 设 $r=c_0.c_1c_2\cdots c_n,0\leqslant c_i<9,1\leqslant c_n<9$ 是一个有限小数,则

$$r=c_0+\frac{c_1c_2\cdots c_n}{10^n}=c_0+\frac{p_1}{2^s5^t},s\geqslant 0,t\geqslant 0,(p_1,2^s5^t)=1$$

因而 $$r=\frac{p}{q},p=c_0q+p_1,q=2^s5^t,(p,q)=1$$

(否则 $(p_1,q)=(p-c_0q,q)=(p,q)>1$ 与 $(p_1,q)=1$ 矛盾)

定理4.2.2 有理数 $r=\dfrac{p}{q},0<p<q,(p,q)=1$ 是一个纯循环小数的充分必要条件是

$$(q,10)=1$$

证明 (1) 设 r 是一个纯循环小数,则

$$r = c_0.\dot{c}_1c_2\cdots\dot{c}_m = c_0.c_1c_2\cdots c_mc_1c_2\cdots c_m\cdots$$

又设 $M = c_1c_2\cdots c_m$，则

$$r = c_0 + \frac{M}{10^m} + \frac{M}{10^{2m}} + \cdots = c_0 + \frac{M}{10^m}\left(1 + \frac{1}{10^m} + \cdots\right) =$$

$$c_0 + \frac{M}{10^m}\cdot\frac{1}{1 - \frac{1}{10^m}} =$$

$$c_0 + \frac{M}{10^m - 1} = \frac{M}{10^m - 1} = \frac{p}{q},(p,q) = 1$$

由于

$$(10^m - 1,10) = (10^m - 1,10^{m-1}.10 - (10^m - 1)) = (10^m - 1,1) = 1$$

q 是 $10^m - 1$ 的因子，故 $(q,10) = 1$。（假若不然，设 $(q,10) = d > 1$，则由于 q 是 $10^m - 1$ 的因子，故 $10^m - 1 = qk$，因而 $(10^{m-1},10) = (qk,10) = d\left(\frac{q}{d}k,\frac{10}{d}\right) \geqslant d > 1$，与 $(10^m - 1,10) = 1$ 矛盾。）

(2) 设 $(q,10) = 1$。则由欧拉定理知存在正整数 n 使得

$$10^n \equiv 1(\bmod q)$$

因此

$$(10^n - 1)p = mq,10^np = p + mq$$

且由于 $mq = 10^np - p < 10^np$，故

$$0 < m < 10^n\cdot\frac{p}{q} < 10^n\left(1 - \frac{1}{q}\right) < 10^n - 1$$

令

$$m = 10m_1 + c_n,0 \leqslant c_n \leqslant 9$$
$$m_1 = 10m_2 + c_{n-1},0 \leqslant c_{n-1} \leqslant 9$$
$$\vdots$$
$$m_{n-1} = 10m_n + c_1,0 \leqslant c_1 \leqslant 9$$

则

$$m = 10^nm_n + 10^{n-1}c_1 + \cdots + 10c_{n-1} + c_n$$

由于 $0 < m < 10^n - 1$，故必须有 $m_n = 0$，且 $c_1,c_2,\cdots,c_n$ 不全为 0，也不全为 9（因为如果全为 0，则 $m = 0$，如果全为 9，则 $m = 10^n - 1$，都与 $0 < m < 10^n - 1$ 矛盾）。因此

$$\frac{m}{10^n} = 0.c_1c_2\cdots c_n$$

由 $10^np = p + mq$ 得出

$$10^n\frac{p}{q} = m + \frac{p}{q}$$

$$\frac{p}{q} = \frac{m}{10^n} + \frac{1}{10^n}\cdot\frac{p}{q}$$

把 $\frac{m}{10^n} = 0.c_1c_2\cdots c_n$ 代入到 $\frac{p}{q} = \frac{m}{10^n} + \frac{1}{10^n}\cdot\frac{p}{q}$ 中去，并反复应用这两个式

子即得

$$\frac{p}{q} = 0.c_1c_2\cdots c_nc_1c_2\cdots c_n\cdots = 0.\dot{c}_1c_2\cdots\dot{c}_n$$

故 r 是一个纯循环小数。

定理 4.2.3 有理数 $r=\frac{p}{q},0<p<q,(p,q)=1$ 是一个混循环小数的充分必要条件是

$$q = 2^\alpha\cdot 5^\beta\cdot\gamma,\alpha\geqslant 0,\beta\geqslant 0$$

且 α,β 不同时为 0，γ 的素因子不同于 2,5。

证明 设

$$A = \left\{r=\frac{p}{q}\,\middle|\,0<p<q,(p,q)=1\right\}$$

则 $A=A_1\cup A_2\cup A_3$，其中 $A_1=\{r\mid r\text{ 是有限小数}\}$，$A_2=\{r\mid r\text{ 是纯循环小数}\}$，$A_3=\{r\mid r\text{ 是混循环小数}\}$，显然，$A_1,A_2,A_3$ 两两不相交。

如果 r 是混循环小数，则由定理 4.2.1 和定理 4.2.2 可知必有 $(q,10)>1$，且 q 中必含有不同于 2,5 的素因子，所以 $q=2^\alpha\cdot5^\beta\cdot\gamma,\alpha\geqslant0,\beta\geqslant0$，且 α,β 不同时为 0，γ 的素因子不同于 2,5。

反过来，如果 $q=2^\alpha\cdot5^\beta\cdot\gamma,\alpha\geqslant0,\beta\geqslant0$，且 α,β 不同时为 0，γ 的素因子不同于 2,5。那么 $(q,10)>1$，因此同样根据定理 4.2.1 和定理 4.2.2 可知 r 既不可能是有限小数，也不可能是纯循环小数，因此必为混循环小数。

上面我们给出了有理数 r 为有限小数，纯循环小数和混循环小数的充分必要条件。下面我们进一步考虑混循环部分的长度和循环节的长度问题。

定理 4.2.4 设 $r=\frac{p}{q},0<p<q,(p,q)=1$ 是一个混循环小数，$q=2^\alpha\cdot5^\beta\cdot\gamma,\alpha\geqslant0,\beta\geqslant0$ 且 α,β 不同时为 0，γ 的素因子不同于 2,5。

则 r 的小数点后不循环部分的长度为 $\max(\alpha,\beta)$。

证明 设 $\alpha\geqslant\beta$，那么

$$10^\alpha\frac{p}{q} = 10^\alpha\frac{p}{2^\alpha5^\beta\gamma} = \frac{5^{\alpha-\beta}p}{\gamma} = M+\frac{p'}{\gamma}$$

其中 $p'<\gamma,0\leqslant M<10^\alpha$，且 $p'=5^{\alpha-\beta}p-M\gamma$，因此

$$(p',\gamma) = (5^{\alpha-\beta}p-M\gamma,\gamma) = (5^{\alpha-\beta}p,\gamma) = 1$$

因而由定理 4.2.2 知 $\frac{p'}{\gamma}$ 是一个纯循环小数：$0.\dot{c}_1c_2\cdots\dot{c}_n$。再设

$$M = a_110^{\alpha-1}+a_210^{\alpha-2}+\cdots+a_\alpha$$

则

$$r = 0.a_1a_2\cdots a_\alpha\dot{c}_1c_2\cdots\dot{c}_n$$

我们还要证明，r 的不循环部分的长度不可能小于 α。假设不然，又有

$$r=\frac{p}{q}=0.b_1b_2\cdots b_\mu\dot{d}_1d_2\cdots\dot{d}_n,0<\mu<\alpha$$

则由定理4.2.2得出

$$10^\mu\frac{p}{q}-\left[10\mu\frac{p}{q}\right]=0.\dot{d}_1d_2\cdots\dot{d}_n=\frac{p'_1}{q'}$$

其中$(q',10)=1$,故

$$10^\mu\frac{p}{q}=\left[10\mu\frac{p}{q}\right]+\frac{p'_1}{q'}=\frac{p'}{q'}$$

或 $$10^\mu pq'=p'q=p'2^\alpha5^\beta\gamma$$

因而 $$2^\alpha\mid 10^\mu pq'$$

上式左边的p,q'都与2互素(因为$(p,q)=(p,2^\alpha5^\beta\gamma)=1,(q',10)=1$),因此必有

$$2^\alpha\mid 10^\mu$$

由于$0<\mu<\alpha$,故这是不可能的,所得的矛盾就证明了r的不循环部分的长度不可能小于α,因而只能是$\alpha=\max(\alpha,\beta)$。

定理4.2.5 设$r=\frac{p}{q},0<p<q,(p,q)=1,(q,10)=1$是一个纯循环小数,则$r$的循环节长度$m\mid\varphi(q)$.

证明 由定理4.2.2(2)的证明知,如果$10^n\equiv1(\bmod q)$,则r的小数点后的n位数字是循环的。设r的循环节的长度是m,那么由$(q,10)=1$及欧拉定理知$10^{\varphi(q)}\equiv1(\bmod q)$,因此由循环节的定义即得$m\mid\varphi(q)$。

由定理4.2.1～定理4.2.3立刻得出:

定理4.2.6 任何无限不循环小数都是无理数。

定义4.2.1 有限小数、循环小数(纯循环小数和混循环小数)以及无限不循环小数的全体称为实数。

定理4.2.7 全体实数和数轴上的点是1—1对应的。

证明 由于数轴的负半轴和正半轴是对称的,因此不妨只考虑全体正实数和数轴的正半轴,在数轴上取定单位长后,任给一个正实数α,设$\alpha=c.c_1c_2\cdots c_n\cdots$,其中$c$是一个正整数,那么按照单位长,正实数就对应了正半轴上的一个点M,反过来,在正半轴上给定了一个点M后,用单位长度去度量OM的长度,就得到一个有限或无限小数,这个小数就对应了一个实数。

按照度量的过程就可知道,如果$\alpha_1<\alpha_2$,那么α_1所对应的点M_1必在α_2所对应的点M_2的左边,即如果$\alpha_1\neq\alpha_2$,则$M_1\neq M_2$。反过来,如果$M_1\neq M_2$,那么不妨设M_1位于M_2的左边,那样按照度量的过程可知M_1所对应的实数α_1必小于M_2所对应的实数α_2,因此$\alpha_1\neq\alpha$,这就说明了这个对应是1—1的。

习题 4.2

1. 把下列循环小数化成分数

(1)$0.\dot{8}$　　(2)$0.\dot{7}\dot{5}$　　(3)$6.\dot{1}4285\dot{7}$

(4)$1.3\dot{8}$　　(5)$0.3\dot{4}\dot{8}$　　(6)$0.17\dot{2}\dot{1}$

2. 求下列各数的小数表示的循环节的长度

(1) $\frac{1}{66}$　　(2) $\frac{1}{666}$　　(3) $\frac{1}{4\,608}$

(4) $\frac{1}{925}$　　(5) $\frac{1}{101}$　　(6) $\frac{1}{1\,001}$

3. 以 2 为基时，求下列各数的小数表示式

(1) $\frac{1}{3}$　　(2) $\frac{1}{5}$　　(3) $\frac{1}{9}$

4. 以 12 为基时，下列各数的小数表示式中，循环节的长度是多少？

(1) $\frac{1}{7}$　　(2) $\frac{1}{11}$　　(3) $\frac{1}{17}$

5. 以 12 为基时，求下列各数的小数表示式

(1) $\frac{1}{13}$　　(2) $\frac{1}{14}$

6. 求下列各数在指定的基下的小数表示式

(1) 以 10 为基，$\frac{1}{9^2}$　　(2) 以 8 为基，$\frac{1}{7^2}$　　(3) 以 7 为基，$\frac{1}{6^2}$

(4) 猜想一个定理

(5) 证明这个定理

7. 证明：有理数化成小数后，其循环节的长度与分子无关。

8. 设 q 为素数，分数 $\frac{p}{q}$，$(p,q)=1$ 生成一个循环节长度为 $2n$ 的小数，那么它的循环节中的前 n 位数字和后 n 位数字之和等于 $99\cdots9$（共有 n 个 9）。

9. 设 $(a,b)=1$，$(a,10)=1$，$(b,10)=1$，以 a 为分母的即约分数生成的小数中循环节的长度为 m，以 b 为分母的即约分数生成的小数中循环节的长度为 n，那么以 ab 为分母的即约分数生成的小数中循环节的长度为 $[m,n]$。特别，以 a 为分母的即约分数之和以 b 为分母的即约分数之和所生成的小数中循环节的长度为 $[m,n]$。

10. 哪些数为分母的即约分数所生成的小数中循环节的长度分别为 1,2,3？

11. 求出所有的数 q，使得以 q 为分母的即约分数生成的混循环小数中，不循环部分的长度为 2，而循环节的长度为 3。

12. 设 $\frac{p}{q}$ 生成循环节长度为 $q-1$ 的纯循环小数，那么 $\frac{1}{q},\frac{2}{q},\cdots,\frac{q-1}{q}$ 中任

一个分数所生成的纯循环小数中循环节中的数字只不过是其他小数的循环节中的数字的一个轮换，因此对这些分数只须计算一个分数所生成的循环小数，就可写出其他分数所生成的循环小数。对 q 等于 7,17,19,23,29,47,59,61 和 97 验证这一现象。

13. 证明：用形如 $\frac{1}{2^n}$ 的分数之和，可以任意逼近一个小于 1 的分数。例如，要近似地分成60等份，可先分成64等份，再加上每一等份的 $\frac{1}{16}$，再加上这 $\frac{1}{16}$ 的 $\frac{1}{16}$。即

$$\frac{1}{64}+\frac{1}{64}\cdot\frac{1}{16}+\frac{1}{64}\cdot\frac{1}{16}\cdot\frac{1}{16}\approx\frac{1}{60}$$

用此方法求一个圆内接正 7 边形的近似做法。

14. 在中古时期即使乘法也不是一般人所能掌握的技巧。但是对不会做乘法运算的印度农民，他们自己摸索出了一种计算两个数相乘的方法如下：

设要计算两个正整数 a,b 的乘积，可令 $a_1=a,b_1=b$，然后在这两个数下面写下一连串数如下图

$$\begin{array}{lll} a_1 & b_1 & \\ a_2 & b_2 & \\ a_{i_1} & b_{i_1} & * \\ \cdots & & \\ a_{i_2} & b_{i_2} & * \\ \cdots & & \\ a_n & b_n=1 & * \end{array}$$

其中，$a_n=2a_{n-1}$，$b_n=\frac{b_{n-1}}{2}$，在 b_{n-1} 不能被 2 除净时，就把余数弃掉，并在 b_{n-1} 的旁边记上一个 * 号，在最后得到的 $b_n=1$ 的旁边也记上一个 * 号，那么要算的乘积就等于把 * 号所在的行中的各个 a_{i_k} 项加起来所得的和数，也即

$$ab=a_{i_1}+a_{i_2}+\cdots+a_{i_k}+a_n$$

例如，要算 78 × 65，可写

78	65	*
156	32	
312	16	
624	8	
1 248	4	
2 496	2	
4 992	1	*

于是 $$78 \times 65 = 4\,992 + 78 = 5\,070$$

证明这一算法的合理性。

15.(1) 设 a 和 b 都是正整数，证明：a 的尾数如果是若干个 0 时，a^2 的尾数必定是偶数个 0，而 $10b^2$ 的尾数如果是若干个 0 时，$10b^2$ 的尾数必定是奇数个 0，利用这一结论证明 $\sqrt{10}$ 是无理数；

(2) 设正整数 b 不是一个完全平方数，考虑整数的以 b 为基的表示式，仿照 (1) 写出一个类似的命题，利用此命题证明 $\sqrt{b}$ 是无理数；

(3) 设 b 不是一个 m 次幂，$m = 3,4,5,\cdots$，用同样的论证说明 $\sqrt[m]{b}$ 是无理数。

16. 证明：$\sum\limits_{n=1}^{\infty} 7^{-\frac{n(n+1)}{2}}$ 是无理数。

4.3　循环小数的一个应用

我们来看一个问题。

例 4.3.1　设 $abcde$ 表示一个 5 位数，已知 $1abcde \times 3 = abcde1$，求 a,b,c,d,e 各是多少。

解法 1　我们从最直接的想法出发，首先想到可以从 e 开始，一个一个地把这些数凑出来。把上面的横式写成竖式。

$$\begin{array}{r} 1\,a\,b\,c\,d\,e \\ \times \qquad\quad 3 \\ \hline a\,b\,c\,d\,e\,1 \end{array}$$

由上面的竖式看出，e 必须是 7，因而 d 需加上进位的 2，因此得到下式

$$\begin{array}{r} 1\,a\,b\,c\,d\,7 \\ \times \qquad\quad {}^{2}3 \\ \hline a\,b\,c\,d\,7\,1 \end{array}$$

由上式看出 $3d + 2 = 17$，因此得出 $d = 5$，进位 1，把 $d = 5$ 代入上式后，又得到下式

$$\begin{array}{r} 1\,a\,b\,c\,5\,7 \\ \times \qquad {}^{1\,2}3 \\ \hline a\,b\,c\,5\,7\,1 \end{array}$$

由上式看出 $3c + 1 = 25$，因此得出 $c = 8$，进位 2，把 $c = 8$ 代入上式后，又

得到下式

$$\begin{array}{r} 1\,a\,b\,8\,5\,7 \\ \times \qquad {}^{2\,1\,2}\,3 \\ \hline a\,b\,8\,5\,7\,1 \end{array}$$

由上式看出 $2b+2=8$,因此得出 $b=2$,没有进位,把 $b=2$ 代入上式后,又得到下式

$$\begin{array}{r} 1\,a\,2\,8\,5\,7 \\ \times \qquad {}^{2\,1\,2}\,3 \\ \hline a\,2\,8\,5\,7\,1 \end{array}$$

从上式最后看出 $a=4$。

用这个办法虽然可以把答案凑出来,但是实在是有点麻烦。其原因就在于用这个方法解题时,是把数字 a,b,c,d,e 都看成一个一个单个的数字,而没有把 $abcde$ 看成一个整体。现面我们看看如果把 $abcde$ 看成一个整体,是不是能有更简便的解法。

解法 2 设5 位数 $abcde=x$,那么由题意可以列出方程

$$3(100\,000+x)=10x+1$$

由此得出

$$7x=299\,999$$

$$x=42\,857$$

因此 $a=4,b=2,c=8,d=5,e=7$。

两相对比,第二种解法就显得简单多了,那么这是不是就是最好的方法了呢,我们说对上面这个问题,这可能就是最简单的方法了,但是对更一般的问题,它又不见得是最好的。

我们再来看一个问题。

例 4.3.2 一个数的个位数是 3,如果把它换到这个数字的首位,那么所得的新数就比原数大一倍,求这个数。

例 4.3.2 和例 4.3.1 很像,其差别就在于不知道所求的数的位数。你别看只少知道这么一点信息,问题的难度就差得很远,这时无论你再用刚才解题时用的解法 1 还是解法 2,都有一种不确定性和心里没有底的感觉。尤其是第一种解法,明显地带有碰运气的成分,在已知原数是 6 位数的情况下,你还有点熬头,反正算到第 5 个数就可见分晓,而现在在不知道位数的情况下,你就不知道要熬到哪年哪月了,看不到希望的日子可是最难熬的啊。

再看第二种解法:

设这个数有 n 位，于是这个 $3\times10^{n-1}+x=2(10x+3)$ 数是 $a_1a_2\cdots a_{n-1}3$，再设

$$x=a_1a_2\cdots a_{n-1}$$

于是根据题意可以列出方程

$$19x=3\times10^{n-1}-6$$

虽然在此之前，我们还一直发挥着这个方法的优越性，但是化到上面的式子后，我们要干的事就变成了做除法

$$299\cdots994\div19$$

至于除到什么时候算完呢？由于不知道 n 是多少，也就是不知道有多少个 9，所以我们的命运就和第一种方法差不多了，也陷入了等待除尽的黑暗中。不信你去算一下，恐怕没有耐心的人是不一定熬得下去的。

那么有没有好一点的办法呢。从上面那道题我们可知原数是 142 857。对这个数，好多人一定不陌生，因为它就是$\frac{1}{7}$ 的循环节。你看，原来那么长的数字，化成分数后却很简单，所以由此受到启发，我们可以设想是不是也可以把这道题里原来的数 $a_1a_2\cdots a_{n-1}3$ 也看成一个小数的循环节而使问题的解法得到简化呢？我现在不能肯定地回答，而只能说，可以试一试，可以说，这是我们在解决任何新的问题时的态度，就是不断地试验和探索，而解决问题的办法就是在这不断的试验和探索中产生的：

设这个数有 n 位，于是这个数是 $a_1a_2\cdots a_{n-1}3$，再设 $x=a_1a_2\cdots a_{n-1}$，于是根据题意可以列出方程

$$3\times10^{n-1}+x=2(10x+3)$$
$$19x=3\times10^{n-1}-6$$
$$x=\frac{3\times10^{n-1}-6}{19}$$

又设 $\alpha=0.\dot{a}_1a_2\cdots a_{n-1}\dot{3}$ 是以 $a_1a_2\cdots a_{n-1}3$ 为循环节的纯循环小数，那么根据我们在前面一节中所讲的把纯循环小数化为分数的方法可知

$$\alpha=\frac{a_1a_2\cdots a_{n-1}3}{10^n-1}=\frac{10x+3}{10^n-1}=\frac{10\cdot\frac{3\cdot10^{n-1}-6}{19}+3}{10^n-1}=$$
$$\frac{3\cdot10^n-60+57}{10^n-1}=\frac{3(10^n-1)}{19(10^n-1)}=\frac{3}{19}=$$
$$0.\dot{1}5789473684210526\dot{3}$$

故所求的数为 157 894 736 842 105 263。

在这个解法里，把我们最烦人，最担心的不知道 n 是多少的问题，通过两种不同的设未知数的方法自动消去了，而且最后连方程也不用解了。问题最后化

为把分数化为循环小数的直接计算问题了。虽然计算仍很烦(由于问题的解本来就是一个 18 位数,所以任何解法都不可能避免导致计算 18 位数的问题)。但是我们心中有底了,我们知道这是一个一定可以算出来的问题,而且由上一节的内容可知,到底要算多少位也是可以估计的。

有的人说,那你这个方法的最后一步中,能从分子分母中把 10^n-1 约去不是也有点凑巧吗?回答是,这回不是凑巧了,而是正体现了这个方法的优越性,如果能约去,就说明问题有解,否则,就说明问题无解。所以说,用这种方法不但能求出问题的解来,而且在求的过程中也就回答了问题是否有解。

4.4 整系数多项式方程的有理根

有理数的特性还可以通过它是否能成为一个多项式方程的根来表现,由于所有的有理系数多项式都可以化成整系数多项式,所以我们可以只限于讨论整系数多项式。

我们有以下的定理:

定理 4.4.1 设 $f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n$ 是整系数多项式,那么如果有理数 $\frac{p}{q}$ 是 $f(x)$ 的根,其中 p,q 是互素的整数,$q\neq 0$,则必有 $p\mid a_n$,$q\mid a_0$。

证明 由于 $\frac{p}{q}$ 是 $f(x)$ 的根,故将其代入方程 $f(x)=0$ 后即得

$$a_0\left(\frac{p}{q}\right)^n+a_1\left(\frac{p}{q}\right)^{n-1}+\cdots+a_n=0$$

$$a_0p^n+a_1p^{n-1}q+\cdots+a_nq^n=0$$

由此得到

$$a_0p^n=-q(a_1p^{n-1}+\cdots a_nq^{n-1})$$

$$p(a_0p^{n-1}+\cdots+a_{n-1}q^{n-1})=-a_nq^n$$

这说明

$$p\mid a_nq^n,q\mid a_0p^n$$

但是因为 $(p,q)=1$,因此 $(p,q^n)=1$,$(p^n,q)=1$,由这两个式子和上面两式就得出

$$p\mid a_n,q\mid a_0$$

作为这一定理的特殊情况,我们有

定理 4.4.2 设 $f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n$ 是整系数多项式,那么如果 $f(x)$ 存在整数根 r,则必有 $r\mid a_n$。

例 4.4.1 解方程 $2x^3+7x^2+4x-3=0$。

证明 如果此方程有一个有理根，那么就可以把它化成为一个一次方程和一个二次方程来解。根据定理 4.4.1，此方程的有理根的分母必是 2 的因数，分子必是 3 的因数，因此它如果存在有理根，则必在 $\pm 1, \pm 3, \pm \frac{1}{2}, \pm \frac{3}{2}$ 这几个数之中。这就把是否存在有理根的问题化为有限次的检验手续了。通过检验发现 $-\frac{3}{2}$ 是此方程的有理根。由于对此方程，我们只须知道一个有理根，就一定可以把它解出来了，所以没有必要再检验其他的数了。因此检验工作可以到此为止。由于 $-\frac{3}{2}$ 是此方程的有理根，因此原方程左端必可被 $2x+3$ 所整除，因而通过长除法就可得出

$$2x^3 + 7x^2 + 4x - 3 = (2x+3)(x^2+2x-1)$$

再解二次方程 $x^2 + 2x - 1 = 0$，即可得出原方程的根为 $-\frac{3}{2}$ 和 $-1 \pm \sqrt{2}$。

例 4.4.2 试证：$x^3 - 3x + 1 = 0$ 不可能分解为有理系数多项式的乘积。

证明 因为原式是 3 次式，所以如果可以分解，则分解的结果必为一个一次式和一个二次式之积，因而必有有理根。这个有理根根据定理 4.4.1 只可能是 1 或 -1。通过检验它们都不是原式的根，因此所说的分解是不可能的。

由此例得出 $x^3 - 3x + 1 = 0$ 的实数根必是无理数。设 $f(x) = x^3 - 3x + 1 = 0$，则 $f(0) = 1 > 0, f(1) = -1 < 0$，因此由连续函数的中间值性质知 $x^3 - 3x + 1 = 0$ 肯定有实数根。这就给出了无理数的具体例子。

例 4.4.3 证明：$\sqrt{2}$ 是无理数。

证明 由$\sqrt{2}$ 的定义知$\sqrt{2}$ 必满足方程 $x^2 - 2 = 0$。因此如果$\sqrt{2}$ 是有理数，那么方程 $x^2 - 2 = 0$ 就必有有理根。然而根据定理 4.4.1，此方程的有理根只可能是 ± 1 和 ± 2，而通过检验可知它们都不是方程 $x^2 - 2 = 0$ 的根。这就证明了$\sqrt{2}$ 是无理数。

上面的例子中多项式的次数都比较低，所以多项式能否分解为有理系数多项式的乘积的问题可以化为多项式是否存在有理根的问题。对一般情况就没有这么简单了，而且也不存在一般的判断法则。以下我们给出一些必要条件以得出一些判断法。

定义 4.4.1 设 $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$ 是一个整系数多项式。如果 $a_0, a_1, \cdots, a_n$ 的最大公因数是 1，则称 $f(x)$ 是一个本原多项式。

显然任何一个有理系数系数多项式都可以化为一个整数和一个整系数多项式的乘积，而任何一个整系数多项式的系数如果有公因数的话，则在提出它们的最大公因数后就得到一个本原多项式，所以任何一个整系数多项式又可以化为一个整数和一个本原多项式的乘积。所以要讨论有理系数系数多项式的分解问题，即分解为有理系数系数多项式的乘积问题，只要讨论本原多项式的分

解问题就可以了。下面我们给出本原多项式的一些性质。

引理 4.4.1 设 p 是一个素数

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$$
$$g(x) = b_0x^m + b_1x^{m-1} + \cdots + b_m$$

是两个整系数多项式。如果 p 整除 $f(x)g(x)$ 的所有系数，则 p 整除 $f(x)$ 的所有系数或 $g(x)$ 的所有系数。

证明 用反证法，假设引理不成立，那么 p 既不整除 $f(x)$ 的所有系数也不整除 $g(x)$ 的所有系数。从后往前看(即从右向左看)，设 a_i 是 $f(x)$ 的系数中第一个不能被 p 整除者。b_j 是 $g(x)$ 的系数中第一个不能被 p 整除者。

于是

$$p \nmid a_i, p \mid a_{i+1}, \cdots, p \mid a_n$$
$$p \nmid b_j, p \mid b_{j+1}, \cdots, p \mid b_m$$

$f(x)g(x)$ 中 $x^{n-i+m-j}$ 的系数是

$$c_{i+j} = \cdots a_{i-2}b_{j+2} + a_{i-1}b_{j+1} + a_ib_j + a_{i+1}b_{j-1} + a_{i+2}b_{j-2} + \cdots$$

在上面的式子中，除 a_ib_j 外的所有项都可以被 p 整除，但是 a_ib_j 这一项不能被 p 整除，否则由 $p \mid a_ib_j$ 将得出 $p \mid a_i$ 或者 $p \mid b_j$，而这与我们的假设矛盾。这就说明 $f(x)g(x)$ 中 $x^{n-i+m-j}$ 项的系数 c_{i+j} 不能被 p 整除，而这又与我们的假设相矛盾。所得的矛盾就证明了引理。

引理 4.4.2 两个本原多项式的乘积仍是一个本原多项式。

证明 设

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$$
$$g(x) = b_0x^m + b_1x^{m-1} + \cdots + b_m$$

是两个本原多项式，因而首先是两个整系数多项式。那么它们的乘积 $f(x)g(x)$ 显然也是一个整系数多项式。如果 $f(x)g(x)$ 不是本原多项式，那么它的所有系数的最大公因数就大于 1，因此存在一个素数 p 整除 $f(x)g(x)$ 的所有系数。根据引理 4.4.1，p 整除 $f(x)$ 的所有系数或 $g(x)$ 的所有系数。这就说明 $f(x)$ 不是本原多项式或者 $g(x)$ 不是本原多项式。而这与假设矛盾，因此 $f(x)g(x)$ 必是本原多项式。

引理 4.4.3 设整系数多项式 $f(x)$ 可以分解为两个有理系数多项式 $f_1(x)$ 与 $f_2(x)$ 的乘积 $f(x) = f_1(x)f_2(x)$，且 $f_1(x)$ 与 $f_2(x)$ 的次数都大于 0，则 $f(x)$ 必可以分解为两个整系数多项式的乘积，而且每一个因子的次数也都大于 0。

证明 不妨设 $f(x)$ 为本原多项式，否则提出它的系数的最大公因数后，$f(x)$ 可表为一个整数和一个本原多项式的乘积，显然，如果原多项式可以分解为两个有理系数多项式的乘积的话，那么这个本原多项式也可以分解为两个有理系数多项式的乘积。

设 m_1 表示 $f_1(x)$ 的系数的公分母，m_2 表示 $f_2(x)$ 的系数的公分母。则 $m_1f_1(x)$ 是整系数多项式，再设 d_1 表示 $m_1f_1(x)$ 的系数的最大公因数，于是 $g_1(x)=\dfrac{m_1f_1(x)}{d_1}$ 是本原多项式，同理，可取 d_2 使 $g_2(x)=\dfrac{m_2f_2(x)}{d_2}$ 是本原多项式。

从 $f(x)=f_1(x)f_2(x)$ 得出

$$\frac{m_1m_2}{d_1d_2}f(x)=g_1(x)g_2(x)$$

设$\dfrac{m_1m_2}{d_1d_2}=\dfrac{p}{q}$，其中 p,q 是互素的正整数，且 $q\neq 0$。则

$$\frac{p}{q}f(x)=g_1(x)g_2(x)$$

由于 $g_1(x),g_2(x)$ 都是本原的，故由引理 4.4.2 知$\dfrac{p}{q}f(x)=g_1(x)g_2(x)$ 也是本原的，因而是整系数多项式。因此 $q\mid pf(x)$，而由于 p,q 是互素的，因此 q 可以整除 $f(x)$ 的所有系数。但因为 $f(x)$ 是本原的，因此 q 必须等于 1，于是

$$pf(x)=g_1(x)g_2(x)$$

如果 $p\neq 1$，那么由于 p 整除 $g_1(x)g_2(x)$ 的所有系数，因而整除 $g_1(x)$ 的所有系数或者 $g_2(x)$ 的所有系数，则得出 $g_1(x)$ 不是本原的或 $g_2(x)$ 不是本原的，而这与假设相矛盾，所以必有 $p=1$。这就证明了引理。

下面给出一个判别法。

定理 4.4.3（爱森斯坦判别法） 设 $f(x)=c_0x^n+c_1x^{n-1}+\cdots+c_n$ 是一个整系数多项式。如果存在素数 p 使得

$$p\nmid c_0,\ p\mid c_1,\cdots,p\mid c_n,\ p^2\nmid c_n$$

则 $f(x)$ 不可能分解为有理系数多项式的乘积。

爱森斯坦（Eisenstein, Ferdinand Gotthold Max, 1823—1852），德国数学家。生于柏林，卒于同地。

证明 由引理 4.4.3，我们只须证明 $f(x)$ 不可能分解为整系数多项式的乘积即可。用反证法。假设 $f(x)=f_1(x)f_2(x)$，而

$$f_1(x)=a_0x^m+a_1x^{k-1}+\cdots+a_k$$
$$f_2(x)=b_0x^k+b_1x^{m-1}+\cdots+b_m$$

都是整系数多项式，且 $m>0,k>0,n=m+k$。

由于 $p\nmid c_0$，$c_0=a_0b_0$，因此 $p\nmid a_0$，$p\nmid b_0$。又因为 $p\mid c_n$，$c_n=a_mb_k$，$p^2\nmid c_n$，因此 a_m 和 b_k 之中有一个且仅有一个可被 p 整除。不妨设 $p\mid a_m$，$p\nmid b_k$. 用 s 表示 p 不能整除的 $f_1(x)$ 的系数的最大下标，因此 $0\leqslant s\leqslant m-1$，$p\nmid a_s$，$p\mid a_{s+1},\cdots,p\mid a_m$。

现在看 $f(x)$ 中 x^{m-s} 项的系数 $c_{n-m+s}=a_sb_k+a_{s+1}b_{k-1}+\cdots$。

根据 s 的定义可知 p 是 $a_{s+1},a_{s+2},\cdots,a_n$ 的公因数，所以 p 整除 c_{n-m+s} 中除

去 $a_s b_k$ 之外的所有项。但是由于 $p \nmid a_s, p \nmid b_k$，所以 $p \nmid a_s b_k$。这就说明 p 不能整除 $f(x)$ 中 x^{m-s} 项的系数 c_{n-m+s}。然而按照定理的条件，$f(x)$ 的系数中，不能被 p 整除的唯一的系数只有 c_0，因此 $n - m + s = 0, n = m - s$。由于 $m < n, s \geqslant 0$，故这是不可能的。这个矛盾就说明我们一开始的假设不成立，这就证明了定理。

例 4.4.4 设 p 是一个素数，证明：$f(x) = \dfrac{x^p - 1}{x - 1}$ 不可能分解为两个有理系数多项式的乘积。

证明 $$f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$$
对此多项式无法直接应用爱森斯坦判别法。

设 $x = y + 1$。则

$$f(x) = \frac{x^p - 1}{x - 1} = \frac{(y+1)^p - 1}{y} =$$
$$\frac{y^p + C_p^1 y^{p-1} + \cdots + C_p^k y^{p-k} + \cdots + C_p^{p-1} y + 1 - 1}{y} =$$
$$y^{p-1} + C_p^1 y^{p-2} + \cdots + C_p^2 y + p = g(y)$$

对多项式 $g(y)$ 可以应用爱森斯坦判别法，因此 $g(y)$ 不可能分解为有理系数多项式的乘积。由于如果 $f(x)$ 可以分解，即 $f(x) = f_1(x)f_2(x)$，则 $g(y) = f_1(y+1)f_2(y+1) = g_1(y)g_2(y)$ 也可以分解，所以这就证明了 $f(x)$ 不可能分解为有理系数多项式的乘积。

定义 4.4.2 两个多项式 $f(x), g(x)$ 如果具有关系 $f(x) = cg(x)$ 或者 $g(x) = cf(x)$，其中 c 是一个非零的常数，则称多项式 $f(x), g(x)$ 是相伴的。

定义 4.4.3 设 $g(x) \mid f(x)$，而 $g(x)$ 既不是常数也不是 $f(x)$ 的相伴多项式，则称 $g(x)$ 是 $f(x)$ 的真因式。

定义 4.4.4 如果多项式 $f(x)$ 既不是常数也没有真因式，则称 $f(x)$ 是不可约多项式。

注意：一个多项式是否是不可约的和它的系数在什么范围内取有关。

例如，多项式 $x^2 - 2$ 在有理数范围内是不可约的，在实数范围内就是可约的，实际上 $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$。

定理 4.4.4 在有理数范围内，存在着次数任意高的不可约多项式。

证明 设 $f(x) = x^n - 2$，则利用爱森斯坦判别法可知 $f(x)$ 不可能分解为有理系数多项式的乘积，这就证明了定理。由于存在着任意大的素数，所以利用例 4.4.4 也可以用 $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ 作为例子来证明这个定理。不过如果把定理的结论改为：对任何自然数 n，在有理数范围内都存在 n 次的不可约多项式，这个例子就不能用了。

习题 4.4

1. 求下列多项式的有理根

(1) $x^3-6x^2+15x-14$ (2) $4x^4-7x^2-5x-1$

(3) $x^5+x^4-6x^3-14x^2-11x-3$

2. 证明在有理数范围内，下列多项式都是不可约的

(1) x^4-x^3+2x+1 (2) $x^4+4kx+1$，其中 k 为任意整数

(3) $x^n+(1+x)^m+(1-x)^m, m\leqslant n$ (4) x^p+px+1，其中 p 为奇素数

3. 下列多项式在有理数范围内是否可约

(1) x^2+1 (2) x^4+1 (3) x^6+x^3+1

4. 设 $f(x)$ 是整系数多项式，r 是 $f(x)$ 的整数根，证明：$f(1)$ 和 $f(-1)$ 都是整数，且

$$(1-r)\mid f(1),(1+r)\mid f(-1)$$

5. 设 $f(x)$ 是整系数多项式。证明：如果 $f(0)$ 和 $f(1)$ 都是奇数，则 $f(x)$ 没有整数根。

6. 设 $p_1,p_2,\cdots,p_r$ 是 r 个互不相同的素数，n 是一个大于 1 的整数，证明：$\sqrt[n]{p_1p_2\cdots p_r}$ 是无理数。

7. 在有理数范围内分解因式

(1) x^4+4

(2) $x^{15}+1$

(3) $x^{12}+x^9+x^6+x^3+1$

(4) $x^8-x^7y+x^6y^2-x^5y^3+x^4y^4-x^3y^5+x^2y^6-xy^7+y^8$

8. 设 n 是自然数，但不是 5 的倍数，证明：$x^{4n}+x^{3n}+x^{2n}+x^n+1$ 可被 $x^4+x^3+x^2+x+1$ 整除。

9. 证明：x^4+2x^2+2x+2 不可能表示成两个整系数的二次三项式之积。

10. 设 $f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n$ 是一个整系数多项式。如果 $f(2)$ 和 $f(5)$ 都是 10 的倍数，则 $f(7)$ 也是 10 的倍数。一般的，如果 p,q 互素，且 $f(p)$ 和 $f(q)$ 都是 pq 的倍数，则 $f(p+q)$ 也是 pq 的倍数。

11. (1) 把 $x^4+4x^3-2x^2-12x+9$ 配成一个二次三项式的平方；

(2) 证明：$x^2+y^2+z^2$ 不可能分解成两个形如 $ax+by+cz$ 的一次式的乘积。

12. 设 $f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n$ 是一个整系数多项式。且存在四个不同的整数 α_i 使得 $f(\alpha_i)=1(i=1,2,3,4)$。证明：不存在任何整数 β 使得 $f(\beta)=-1$。

13. 设 a,b,c 是三个不同的整数，$P(x)$ 是一个整系数多项式。证明：不可

能有 $P(a)=b, P(b)=c, P(c)=a$。是否能把这一结论推广到 n 个不同整数的情况？

14. 证明：多项式 $x^{200}y^{200}+1$ 不可能表示为变量分离形式的乘积，即表示成 $f(x)g(y)$ 的形式。

15. 试求出两个常数 a, b 使得 $(2x-1)^{20}-(ax+b)^{20}$ 是一个二次三项式的 10 次方。

16. 已知 a, b, c, d 是互不相同的整数，r 是方程 $(x-a)(x-b)(x-c)(x-d)=9$ 的整数根，求证：$4r=a+b+c+d$。

4.5　实数和极限

在前几节中，我们研究了单个有理数的某些性质，而在这一节里，我们将研究有理数全体作为一个集合的性质。

有理数在有些方面是和整数很相像的，比如说，全体有理数是可数的，但是在有些方面又和整数很不一样，比如说在连续两个整数之间是不存在任何整数的，但是对于有理数却不是这样。我们有

定理 4.5.1　对任何两个有理数 $r_1<r_2$ 之间，都存在着与它们不同的有理数 r，使得

$$r_1<r<r_2$$

证明　取 $r=\dfrac{r_1+r_2}{2}$ 即可。

上面的定理是说，有理数自身是稠密的（与整数对比）。不但如此，我们还有全体有理数在全体实数中也是稠密的。但是为此，我们必须说明什么是实数。

我们复习一下几个概念和结论。

定义 4.2.1　有限小数、循环小数（纯循环小数和混循环小数）以及无限不循环小数的全体称为实数。

定理 4.2.7　（实数的连续性）全体实数和数轴上的点是 1—1 对应的。

有了实数的连续性，今后我们就不再区分数轴上的点和实数，当我们说实数 c 时，我们也指实数 c 在数轴上所代表的点，反过来，当我们说点 c 时，我们也指在数轴上点 c 所表示的实数。

定理 4.5.4　设 α 是任意实数，那么任给 $\epsilon>0$，都存在有理数 r，使得

$$|\alpha-r|<\epsilon$$

证明　设 $\alpha=c.c_1c_2\cdots c_n\cdots$，$r_n=c.c_1c_2\cdots c_n$，那么 r_n 都是有理数，且

$$|\alpha-r_n|=\frac{0.c_{n+1}c_{n+2}\cdots}{10^n}<\frac{1}{10^n}$$

因此,只要 n 足够大,就可使 $|\alpha - r_n| < \frac{1}{10^n} < \varepsilon$。

满足 $|\alpha - r| < \varepsilon$ 的 r 表示数轴上以 α 为中心,以 ε 为半径的区间内的所有点(如下图)



这就是说,在数轴上,任给一个实数 α,从 α 的左边或右边,不论离 α 多近的地方都存在着有理数。

有理数的这个性质是非常好的,正因为有理数具有这个性质,我们在实际中只要用到有理数便可以完成一切实用的计算。如果有理数没有这一性质,那真是不可想象我们将如何计算和生活。

下面,我们引进数列的界和极限的概念。

定义 4.5.2 设 E 是一个点集,如果存在一个正数 $M > 0$,使得对于 E 中的任何一点 x,都有 $|x| \leqslant M$,则称 E 是有界集。

如果对于 E 中的任何一点 x,都有 $x \leqslant M$,其中 M 是某一个实数,则称 M 是 E 的一个上界,类似地,如果对于 E 中的任何一点 x,都有 $x \geqslant M$,其中 M 是某一个实数,则称 M 是 E 的一个下界。

显然,如果一个集合有上界,那么它就有无数个上界,同样,如果一个集合有下界,那么它就有无数个下界。

定义 4.5.3 设给定了一个数列 $\{x_n\}$,如果对任意给定的正数 $\varepsilon > 0$,都存在一个正整数 N,使得当 $n > N$ 时,成立不等式 $|x_n - A| < \varepsilon$,其中 A 是一个实数。就称 A 是当 n 趋于无穷大时,数列 $\{x_n\}$ 的极限,记为 $\lim\limits_{n\to\infty} x_n = A$,或者当 $n \to \infty$ 时,$x_n \to A$。

如果当 $n \to \infty$ 时,数列 $\{x_n\}$ 存在极限,则称数列 $\{x_n\}$ 收敛。

直观地说起来,说 $\lim\limits_{n\to\infty} x_n = A$ 的意思就是当 n 充分大时,$|x_n - A|$ 就可以变得要多小就有多小,或者 x_n 可以距离 A 要多近就有多近。定义中"当 $n > N$ 时"就是"当 n 充分大时"的严格表述,而"对任意给定的正数 $\varepsilon > 0$"和"成立不等式 $|x_n - A| < \varepsilon$"就是"$|x_n - A|$ 就可以变得要多小就有多小,或者 x_n 可以距离 A 要多近就有多近"的严格表述。"因为任意给定的正数 $\varepsilon > 0$"这句话本身就隐含着 $\varepsilon > 0$ 是可以任意小的,而 $|x_n - A|$ 在几何上的意义就是在数轴上 x_n 和 A 之间的距离。

关于极限,有以下一些初等的性质。

定理 4.5.5 数列的极限有以下性质:

(1) 如果当 $n \to \infty$ 时,$x_n \to a > 0$,则存在正整数 N,使得当时 $n > N$ 时,$x_n > 0$;类似的,如果当 $n \to \infty$ 时,$x_n \to a < 0$,则存在正整数 N,使得当 $n > N$

时，$x_n < 0$；

(2) 如果当 $n \to \infty$ 时，$x_n \to a, a \neq 0$，则存在正整数 N，使得当 $n > N$ 时，$|x_n| > r > 0$；

(3) 如果当 $n \to \infty$ 时，x_n 存在极限，则数列 $\{x_n\}$ 是有界的；

(4) 设当 $n \to \infty$ 时，x_n 存在极限，则此极限是唯一的；

(5) 设当 $n \to \infty$ 时，$x_n \to a, y_n \to b$，则当时 $n \to \infty$ 时，$x_n + y_n \to a + b$；

(6) 设当 $n \to \infty$ 时，$x_n \to a, y_n \to b$，则当时 $n \to \infty$ 时，$x_n - y_n \to a - b$；

(7) 设当 $n \to \infty$ 时，$x_n \to a, y_n \to b$，则当时 $n \to \infty$ 时，$x_n \cdot y_n \to a \cdot b$；

(8) 设当 $n \to \infty$ 时，$x_n \to a, y_n \to b$，且 $b \neq 0$，则当 $n \to \infty$ 时，$\frac{x_n}{y_n} \to \frac{a}{b}$；

(9) 设当 $n \to \infty$ 时，$x_n \to a$，$f(x)$ 在点 a 连续，则当 $n \to \infty$ 时，$f(x) \to f(a)$。

证明 (1) 设当 $n \to \infty$ 时，$x_n \to a > 0$，那么根据极限的定义，对 $\frac{a}{2} > 0$ 存在正整数 N 使得当 $n > N$ 时，成立不等式 $|x_n - a| < \frac{a}{2}$，于是 $-\frac{a}{2} < x_n - a < \frac{a}{2}$，$\frac{a}{2} < x_n < \frac{3a}{2}$，这就证明了，当 $n > N$ 时，$x_n > \frac{a}{2} > 0$，同理可以证明，如果 $a < 0$，那么当 $n > N$ 时，$x_n < -\frac{a}{2} < 0$.

(2) 设当 $n \to \infty$ 时，$x_n \to a, a \neq 0$，那么根据极限的定义，对 $\frac{|a|}{2} > 0$ 存在正整数 N 使得当 $n > N$ 时，成立不等式 $|x_n - a| < \frac{|a|}{2}$，于是就有

$$|x_n| = |a + x_n - a| \geqslant |a| - |x_n - a| \geqslant |a| - \frac{|a|}{2} > \frac{|a|}{2} > 0$$

这就证明了(2)。

(3) 设当 $n \to \infty$ 时，x_n 存在极限 a，那么根据极限的定义，对 $|a| + 1 > 0$，存在正整数 N 使得当 $n > N$ 时，成立不等式 $|x_n - a| < |a| + 1$，于是当 $n > N$ 时就有

$$|x_n| = |a + x_n - a| \leqslant |a| + |x_n - a| \leqslant |a| + |a| + 1 \leqslant 2|a| + 1$$

令 $\max(|x_1|, |x_2|, \cdots, |x_N|, 2|a| + 1)$，则对所有的 n 就都成立 $|x_n| \leqslant M$（只要对 $n \leqslant N$ 和 $n > N$ 这两种情况分别验证就可得到不等式 $|x_n| \leqslant M$）。这就证明了 x_n 的有界性。

(4) 假设同时成立 $x_n \to a, x_n \to b, a \neq b$，那么不妨设 $a < b$。又设 $a < r < b$，那么根据极限的定义，对于 $\epsilon = \min(r - a, b - r) > 0$，存在正整数 N_1 使得当 $n > N_1$ 时，成立不等式

$$|x_n - a| < \epsilon \leqslant r - a$$

又存在正整数 N_2,使得当 $n > N_2$ 时,成立不等式

$$|x_n - b| < \varepsilon \leqslant b - r$$

令 $N = \max(N_1, N_2)$,于是当 $n > N$ 时一方面就有

$$|x_n - a| < \varepsilon \leqslant r - a, a - r < x_n - a < r - a$$

因此 $x_n < r$,另一方面又有

$$|b - x_n| = |x_n - b| < \varepsilon \leqslant b - r, r - b < b - x_n < b - r$$

因此又有 $-x_n < -r, x_n > r$,这与 $x_n < r$ 矛盾,所得的矛盾就说明如果数列 $\{x_n\}$ 存在极限,则此极限必定是唯一的。

(5) 设当 $n \to \infty$ 时,$x_n \to a, y_n \to b, \varepsilon > 0$是任意的正数。那么根据极限的定义,对于$\frac{\varepsilon}{2} > 0$,存在正整数 N_1 使得当 $n > N_1$ 时,成立不等式 $|x_n - a| < \frac{\varepsilon}{2}$,又存在正整数 N_2 使得当 $n > N_2$ 时,成立不等式 $|x_n - b| < \frac{\varepsilon}{2}$。令 $N = \max(N_1, N_2)$,于是当 $n > N$ 时就有

$$|(x_n + y_n) - (a + b)| = |(x_n - a) + (y_n + b)| \leqslant$$

$$|(x_n - a)| + |(y_n + b)| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} \leqslant \varepsilon$$

因而由极限的定义就得出当 $n \to \infty$ 时,$x_n + y_n \to a + b$。

(6) 设当 $n \to \infty$ 时,$x_n \to a, y_n \to b$,那么由极限的定义易于得出$(-y_n) \to (-b)$,因而再由(5)已证明的结论就得出

$$x_n - y_n = x_n + (-y_n) \to a + (-b) = a - b$$

(7) 设当 $n \to \infty$ 时,$x_n \to a, y_n \to b, 1 > \varepsilon > 0$是正数。那么根据极限的定义,对于$\frac{\varepsilon}{3|b|+3} > 0$,存在正整数 N_1 使得当 $n > N_1$ 时,成立不等式

$$|x_n - a| < \frac{\varepsilon}{3|b|+3}$$

对于$\frac{\varepsilon}{3|a|+3}$,存在正整数 N_2 使得当 $n > N_2$ 时,成立不等式

$$|y_n - b| < \frac{\varepsilon}{3|a|+3}$$

令 $N = \max(N_1, N_2)$,于是当 $n > N$ 时就有

$$|x_ny_n - ab| = |a(y_n - b) + b(x_n - a) + (x_n - a)(y_n - b)| \leqslant$$

$$|a||y_n - b| + |b||x_n - a| + |x_n - a||y_n - b| <$$

$$\frac{|a|\varepsilon}{3|a|+3} + \frac{|b|\varepsilon}{3|b|+3} + \frac{\varepsilon}{3|a|+3} \cdot \frac{\varepsilon}{3|b|+3} \leqslant$$

$$\frac{\varepsilon}{3} + \frac{\varepsilon}{3} + \frac{\varepsilon}{3} \cdot 1 \leqslant \varepsilon$$

因而由极限的定义就得出当 $n \to \infty$ 时，$x_n \cdot y_n \to a \cdot b$。

(8) 设当 $n \to \infty$ 时，$x_n \to a$，$y_n \to b$，且 $b \neq 0$，$\varepsilon > 0$ 是正数。于是根据(2)已证的结论知存在正整数 N_1 使得当 $n > N_1$ 时，成立不等式 $|y_n| > r > 0$，又对于 $|b| r\varepsilon > 0$ 存在正整数 N_2 使得当 $n > N_2$ 时，成立不等式 $|y_n - b| < |b| r\varepsilon$。因而当 $n > N = \max(N_1, N_2)$ 时成立不等式

$$\left|\frac{1}{y_n} - \frac{1}{b}\right| = \frac{|y_n - b|}{|y_n||b|} < \frac{|b| r\varepsilon}{|b| r} < \varepsilon$$

再由极限的定义就得出当 $n \to \infty$ 时，$\frac{1}{y_n} \to \frac{1}{b}$，因此再由(7)已证的结论就有

$$\frac{x_n}{y_n} = x_n \cdot \frac{1}{y_n} \to a \cdot \frac{1}{b} = \frac{a}{b}$$

这就证明了(8)。

(9) 根据 $f(x)$ 在 a 点连续的定义就得出这一性质。

利用实数的连续性，在本书中我们认为下面的性质是不需证明的基础事实。

实数的基础性质(区间套性质) 设 $a_1 \leqslant a_2 \leqslant \cdots \leqslant a_n \leqslant \cdots \leqslant b_n \leqslant \cdots \leqslant b_2 \leqslant b_1$，且当 $n \to \infty$ 时，$(b_n - a_n) \to 0$，则存在一个唯一的点 c 属于所有的闭区间 $[a_n, b_n]$，点 c 是当 $n \to \infty$ 时，数列 $\{a_n\}$ 和 $\{b_n\}$ 的公共极限，即 $a_n \to c$，$b_n \to c$。

这就好像两个人迎面而行，并且每个人只许前进，不许后退，并要求它们之间的距离趋于零，那么这两个人最后就必然都趋向于它们之间的同一个点。

上面我们所讲的极限的性质都是在假定极限存在的前提下得出的，然而至今我们还没有给出任何能够判断极限是否存在的判据。下面我们就给出这样的判据。

定理 4.5.6(两边夹定理) 设当 $n \to \infty$ 时，$x_n \to c$，$y_n \to c$，且当 n 充分大时成立

$$x_n \leqslant z_n \leqslant y_n$$

则当 $n \to \infty$ 时，$z_n \to c$。

证明 设当 $n \to \infty$ 时，$x_n \to c$，$y_n \to c$，且当 n 充分大时成立 $x_n \leqslant z_n \leqslant y_n$。那么根据极限的定义，对于任意的正数 $\varepsilon > 0$，存在正整数 N_1 使得当 $n > N_1$ 时，成立不等式 $|x_n - c| < \varepsilon$，又存在正整数 N_2 使得当 $n > N_2$ 时，成立不等式 $|y_n - c| < \varepsilon$，还存在正整数 N_3 使得当 $n > N_3$ 时，成立不等式 $x_n \leqslant z_n \leqslant y_n$。于是当 $n > \max(N_1, N_2, N_3)$ 时，我们有 $c - \varepsilon < x_n \leqslant z_n \leqslant y_n < c + \varepsilon$，因而 $|z_n - c| \leqslant \varepsilon$，而由极限的定义，这就说明当 $n \to \infty$ 时，$z_n \to c$。

上面曾提到过如果一个集合有上界，那么它就有无数个上界，同样，如果一

个集合有下界,那么它就有无数个下界。

在所有的上界中,最小的上界特别有用,同样在所有的下界中,最大的下界特别有用。由此引出下面的概念:

定义 4.5.4 设 E 是有上界的集合,那么在 A 的一切上界中最小的上界称为 E 的上确界,记为 $\sup E$;类似的,设 E 是有下界的集合,那么在 E 的一切下界中最大的上界称为 E 的下确界,记为 $\inf E$。

现在发生一个问题,那就是上确界和下确界是否一定存在,对此,有下面的定理:

定理 4.5.7 有上界的集合必存在上确界,有下界的数列必存在下确界。

证明 设 E 有上界 M,在 E 中任取一个元素 u,令 $c_1 = \frac{u+M}{2}$,如果 c_1 是 E 的上界,则令 $a_1 = u, b_1 = c_1$,如果 c_1 不是 E 的上界,则令 $a_1 = c_1, b_1 = M$;再令 $c_2 = \frac{a_1+b_1}{2}$,如果 c_2 是 E 的上界,则令 $a_2 = a_1, b_2 = c_2$,如果 c_2 不是 E 的上界,则令 $a_2 = c_2, b_2 = b_1$;再令 $c_3 = \frac{a_2+b_2}{2}$,如果 c_3 是 E 的上界,则令 $a_3 = a_2, b_3 = c_3$,如果 c_3 不是 E 的上界,则令 $a_3 = c_3, b_3 = b_2$;$\cdots$ 依此类推,乃至无穷。

由闭区间 $[a_n, b_n]$ 的构造过程可知闭区间 $[a_n, b_n]$ 有以下性质:

(1) b_n 总是 E 的上界;

(2) a_n 总不是 E 的上界;

(3) $b_n - a_n = \frac{b_{n-1} - a_{n-1}}{2}$,因而 $b_n - a_n = \frac{b_1 - a_1}{2^{n-1}}$,故当 $n \to \infty$ 时,$(b_n - a_n) \to 0$。

由闭区间 $[a_n, b_n]$ 性质(1) 得出对任意 $x \in E$,$|x| \leqslant b_n$,因而 $|x| \leqslant c$。这就说明 c 是 E 的上界。

由区间套性质知道存在唯一的一个数 c 使得当 $n \to \infty$ 时 $a_n \to c, b_n \to c$。因而由 a_n 递增,b_n 递减和极限的性质得出 n 成立 $a_n \leqslant c \leqslant b_n$。任给正数 $\varepsilon > 0$,根据极限的定义,存在整数 N,使得当 $n > N$ 时,$|a_n - c| < \varepsilon$,故 $c - \varepsilon < a_n \leqslant c$。但是由闭区间 $[a_n, b_n]$ 的性质(2) 又知道对每一个 a_n,总存在着一个 $u_n \in E$,使得 $a_n \leqslant u_n$,因而 $c - \varepsilon < a_n \leqslant u_n$,这说明任何比 c 小的数 $c - \varepsilon$ 都不是 E 的上界,因此 c 就是 E 的上确界。

同理可证定理的另一部分。

定理 4.5.8(维尔斯特拉斯) 设 x_n 是单调递增有上界的数列,那么当 $n \to \infty$ 时,x_n 必趋于一个极限。类似地设 x_n 是单调递减有下界的数列,那么当 $n \to \infty$ 时,x_n 必趋于一个极限。

维尔斯特拉斯(Weierstrass, Karl Theodor Wilhelm, 1815—1897),德国数学家,生于德国西部威斯特伐利里的小村落奥斯滕费尔德,卒于柏林。

证明 由于集合$\{x_n\}$有上界,因此根据定理4.5.6,它必有上确界,设 $a=\sup\{x_n\}$。那么根据上确界的定义,一方面对所有的 n 都成立 $x_n \leqslant a$,另一方面,任给正数 $\epsilon>0$,$a-\epsilon$ 都不可能是$\{x_n\}$的上界(因为如果 $a-\epsilon$ 是$\{x_n\}$的上界,那么由于 $a-\epsilon$ 比 a 小,因此就与 a 是$\{x_n\}$的上确界,即与最小的上界的假设相矛盾)。因此必存在一个 x_N 使得 $a-\epsilon<x_N$,而由于$\{x_n\}$是单调递增的,因此当 $n>N$ 时就有 $a-\epsilon<x_N\leqslant x_n\leqslant a<a+\epsilon$,因而 $|x_n-a|<\epsilon$,而按照极限的定义,这就是说当 $n\to\infty$ 时,$x_n\to a$。类似地可以证明定理的另一部分。

习题 4.5

1. 设是 $x_1,x_2,\cdots,x_n$ 符号相同且大于1的数,证明:

$$(1+x_1)(1+x_2)\cdots(1+x_n)\geqslant 1+x_1+x_2+\cdots+x_n$$

2. 证明:$(1+x)^n\geqslant 1+nx(x>-1)$,且等号仅在 $x=0$ 时成立。

3. 设 $x_1,x_2,\cdots,x_n$ 都是正数,且 $x_1x_2\cdots x_n=1$,证明:$x_1+x_2+\cdots+x_n\geqslant n$。

4. 设 $a_1,a_2,\cdots,a_n$ 都是正数,证明:$\dfrac{a_1+a_2+\cdots+a_n}{n}\geqslant\sqrt[n]{a_1a_2\cdots a_n}$,且等号仅在 $a_1=a_2=\cdots=a_n$ 时成立。

5. 证明:$n!<\left(\dfrac{n+1}{2}\right)^n$。

6. 证明:$2!4!\cdots(2n)!>[(n+1)!]^2$。

7. 证明:$\sqrt[n]{n!}\geqslant\sqrt{n}$。

8. 证明:$\dfrac{1}{2}\cdot\dfrac{3}{4}\cdot\cdots\cdot\dfrac{2n-1}{2n}<\dfrac{1}{\sqrt{2n+1}}$。

9. 设 $M_\gamma(a)=\left(\dfrac{a_1^\gamma+a_2^\gamma+\cdots+a_n^\gamma}{n}\right)^{\frac{1}{\gamma}}$,$M_0(a)=\sqrt[n]{a_1a_2\cdots a_n}$,证明:对任意实数 $\alpha\leqslant\beta$ 成立

$$M_\alpha(a)\leqslant M_\beta(a)$$

等号仅在 $a_1=a_2=\cdots=a_n$ 时成立。

10. 设 $x\geqslant -1$,那么

(1) 当 $0<\alpha<1$ 时有 $(1+x)^\alpha\leqslant 1+\alpha x$;

(2) 当 $\alpha<0$ 或 $\alpha>1$ 时有 $(1+x)^\alpha\geqslant 1+\alpha x$。

等号仅在 $x=0$ 时成立。

11. 设 $a_1,a_2,\cdots,a_n$ 及 $b_1,b_2,\cdots,b_n$ 是任意实数,证明:

$$|a_1b_1+a_2b_2+\cdots+a_nb_n|\leqslant\sqrt{a_1^2+a_2^2+\cdots+a_n^2}\cdot\sqrt{b_1^2+b_2^2+\cdots+b_n^2}$$

等号仅在 $a_1=a_2=\cdots=a_n=0$ 或 $b_1=b_2=\cdots=b_n=0$ 或 $b_1,b_2,\cdots,b_n$ 不全为0,而 $\dfrac{a_1}{b_1}=\dfrac{a_2}{b_2}=\cdots=\dfrac{a_n}{b_n}$(当 $b_i=0$ 时认为 $a_i=0$)时成立。

12. 证明不等式：$|x-y| \geqslant ||x|-|y||$。

13. 证明不等式：

(1) $|x_1+x_2+\cdots+x_n| \leqslant |x_1|+|x_2|+\cdots+|x_n|$；

(2) $|x+x_1+x_2+\cdots+x_n| \geqslant |x|-(|x_1|+|x_2|+\cdots+|x_n|)$。

14. 证明：分数$\frac{a_1+a_2+\cdots+a_n}{b_1+b_2+\cdots+b_n}$在下列各分数$\frac{a_1}{b_1},\frac{a_2}{b_2},\cdots,\frac{a_n}{b_n}(b_k>0,k=1,2,\cdots,n)$中的最大值和最小值之间。

15. 证明：(1) 当 θ 充分小时：$\cos 2\theta < \cos\theta\cos\sqrt{3}\theta$；

(2) 设 $\cos\varphi=\frac{\cos 2\theta}{\cos\theta}$，则当 θ 充分小时 $\varphi>\sqrt{3}\theta$。

16. 证明：当 $n\to\infty$ 时有

(1) $\frac{n}{2^n}\to 0$ (2) $\frac{2^n}{n!}\to 0$ (3) $\frac{n^k}{a^n}\to 0(a>1)$ (4) $\frac{a^n}{n!}\to 0$

(5) $nq^n\to 0(|q|<1)$ (6) $\sqrt[n]{a}\to 1(a>0)$ (7) $\sqrt[n]{n}\to 1$ (8) $\frac{1}{\sqrt[n]{n!}}\to 0$

17. 证明：当 $n\to\infty$ 时$\frac{\log_a n}{n}\to 0(a>1)$。

18. 如果存在数 $C>0$，使得 $|x_2-x_1|+|x_3-x_2|+\cdots+|x_n-x_{n-1}|<C$，则称数列$\{x_n\}$有有界变差。证明：$n\to\infty$ 时有有界变差的数列一定存在极限。

19. 证明：如果叙列$\{x_n\}$收敛，则它的任何子叙列$\{x_n\}$也收敛，且二者具有相同的极限。

20. 证明：如果单调序列的某一子序列收敛，则此单调序列收敛。

21. 设当 $n\to\infty$ 时 $x_n\to a$，则当 $n\to\infty$ 时$\frac{x_1+x_2+\cdots+x_n}{n}\to a$，试举例说明相反的结论不成立。

22. 证明：如果

(1) $y_{n+1}>y_n(n=1,2,3,\cdots)$；

(2) 当 $n\to\infty$ 时，$y_n\to+\infty$；

(3) $\lim\limits_{n\to\infty}\frac{x_{n+1}-x_n}{y_{n+1}-y_n}$ 存在；

则

$$\lim_{n\to\infty}\frac{x_n}{y_n}=\lim_{n\to\infty}\frac{x_{n+1}-x_n}{y_{n+1}-y_n}$$

23. (1) 证明：$\arctan\frac{1}{d}=\arctan\frac{1}{d+1}+\arctan\frac{1}{d^2+d+1}$；

(2) 设

$$a_1 = 1$$

$$a_2 = \frac{1}{2} + \frac{1}{3}$$

$$a_3 = \frac{1}{3} + \frac{1}{7} + \frac{1}{4} + \frac{1}{13}$$

$$a_4 = \frac{1}{4} + \frac{1}{13} + \frac{1}{8} + \frac{1}{57} + \frac{1}{5} + \frac{1}{21} + \frac{1}{14} + \frac{1}{183}$$

$$\vdots$$

其中 a_{n+1} 是把 a_n 中的每个分数 $\frac{1}{d}$ 换成 $\frac{1}{d+1} + \frac{1}{d^2+d+1}$ 而得到的。

证明：当 $n \to \infty$ 时，数列 a_n 存在极限，并求出这个极限来。

24. 设 $x_1 = a > 0, y_1 = b > 0, x_{n+1} = \sqrt{x_n y_n}, y_{n+1} = \frac{x_n + y_n}{2}$，证明：当 $n \to \infty$ 时，数列 x_n 和 y_n 存在相同的极限。

4.6 开集和闭集

为了更深刻地描述有理数的性质，我们下面引进点集的语言。

定义 4.6.1 设 E 是直线上一些点的集合，如果对于一个点 x_0，存在 E 的开区间 (α, β) 使得 $x_0 \in (\alpha, \beta) \subset E$，则称 x_0 是集合 E 的内点。

定义 4.6.2 如果集合 E 的所有点都是它的内点，则称 E 是开集。

由内点的定义看出，E 的内点必属于 E。因此要说明一个集合是开集，只须考虑属于它本身的点就够了。

例 4.6.1

(1) 开区间 (a, b) 是开集；

(2) 全体实数的集合是开集；

(3) 空集是开集；

关于空集为什么也是开集，可能有的读者不理解，这个你可以从如果一个集合不是开集，那么它必有一个点不具有性质 $x_0 \in (\alpha, \beta) \subset E$，但是空集不包含任何点，因此空集中没有不具有性质 $x_0 \in (\alpha, \beta) \subset E$ 的点，因此空集是开集。

(4) 闭区间 $[a, b]$ 不是开集，因为它的两个端点不具有性质 $x_0 \in (\alpha, \beta) \subset E$。

(这里 $E = [a, b]$)

定理 4.6.1 任意个开集的和集是开集。

证明 设 $G=\bigcup_{\xi} G_{\xi}$,其中 G_{ξ} 都是开集。设 $x_0\in G$,则 x_0 必属于某一个 G_{ξ}。由于 G_{ξ} 是开集,因此存在开区间 (α,β) 使得 $x_0\in(\alpha,\beta)\subset G_{\xi}$,因而 $x_0\in(\alpha,\beta)\subset G_{\xi}\subset G$,即 x_0 是 G 的内点。由 x_0 的任意性就知道 G 中的任何点都是内点,故 G 是开集。

由这个定理和例 4.6.1(1) 立刻得出:

定理 4.6.2 如果一个集合 E 可以表示成一些开区间的并集,则 E 是开集。

定理 4.6.3 有限个开集的交集还是开集。

证明 设 $P=\bigcap_{k=1}^{n} G_k$,其中 $G_1,G_2,\cdots,G_n$ 都是开集。

如果 P 是空集,那么 P 就是开集,定理已得证。

如果 P 不是空集,那么对任意 $x_0\in P$,因此 $x_0\in G_k$, $k=1,2,\cdots,n$。对于每一个 k 有一个 (α_k,β_k) 使得 $x_0\in(\alpha_k,\beta_k)\subset G_k$。

令 $\alpha=\max(\alpha_1,\alpha_2,\cdots,\alpha_n)$, $\beta=\min(\beta_1,\beta_2,\cdots,\beta_n)$,则

$$x_0\in(\alpha,\beta)\subset P$$

这就表示 x_0 是 P 的内点,由 x_0 的任意性,就证明了 P 是开集。

注意:无限个开集的交集不一定是开集。例如,设那 $G_n=\left(-\frac{1}{n},\frac{1}{n}\right)$, $n=1,2,3,\cdots$,那么 G_n 都是开集,然而它们的交集

$$P=\bigcap_{n=1}^{\infty} G_n=\{0\}$$

却不是开集。

定义 4.6.3 设 E 是一个点集,x_0 是一个点。如果任何含有 x_0 的开区间除 x_0 之外还至少含有 E 的一点,则称 x_0 是 E 的一个极限点或聚点。

E 中不是极限点的点称为 E 的孤立点。

定理 4.6.4 x_0 是 E 的极限点的充分必要条件是

(1) 包含 x_0 的任意开区间 (α,β) 中必含有 E 的无限个不同的点;

(2) E 中包含一个序列 $\{x_n\}$ ($x_n\neq x_0$,当 $n\neq m$ 时,$x_n\neq x_m$),使得 $\lim\limits_{n\to\infty} x_n=x_0$。

证明 (1) 设 x_0 是 E 的极限点,(α,β) 是包含 x_0 的开区间。那么设

$$\alpha_1=\alpha,\ \beta_1=\beta$$

$$\alpha_2=\frac{\alpha_1+x_0}{2},\ \beta_2=\frac{x_0+\beta_1}{2}$$

$$\vdots$$

$$\alpha_n=\frac{\alpha_{n-1}+x_0}{2},\ \beta_n=\frac{x_0+\beta_{n-1}}{2}$$

$$\vdots$$

则由 α_n,β_n 的定义可知 $\alpha<\alpha_2<\cdots<\alpha_n<\cdots<x_0<\cdots<\beta_n<\cdots<\beta_2<\beta$。于是由极限点的定义可知在开区间 (α,β) 中含有一个 E 中异于 x_0 的点 x_1，在开区间 (α_2,β_2) 中又含有一个 E 中异于 x_0 的点 $x_2,\cdots$，在开区间 (α_n,β_n) 中又含有一个 E 中异于 x_0 的点 $x_n,\cdots$。显然 $x_1,x_2,\cdots x_n,\cdots$ 都是异于 x_0 的点，并且它们本身也都是两两不同的，这就证明了 (α,β) 必包含 E 中无限个不同于 x_0 的点。

反过来，设 x_0 是一个点，包含 x_0 的任意开区间 (α,β) 中含有 E 的无限个不同的点，于是当然 (α,β) 中含有 E 的点，因而根据极限点的定义即知 x_0 是 E 的极限点。

(2) 设 x_0 是 E 的极限点，于是由(1)中的证明可知存在开区间 (α_n,β_n)，使得在 (α_n,β_n) 中存在 E 的点 x_n，而且 $x_1,x_2,\cdots,x_n\cdots$ 都是异于 x_0 的点，并且它们本身也都是两两不同的。

由 (α_n,β_n) 的定义可知

$$\beta_n-\alpha_n=\frac{\beta_{n-1}-\alpha_{n-1}}{2}=\frac{\beta_{n-2}-\alpha_{n-2}}{2^2}=\cdots=\frac{\beta-\alpha}{2^{n-1}}$$

因此

$$|x_n-x_0|<\frac{\beta-\alpha}{2^{n-1}}$$

这就证明了 E 中包含一个序列 $\{x_n\}$（$x_n\neq x_0$，当 $n\neq m$ 时，$x_n\neq x_m$），使得 $\lim\limits_{n\to\infty}x_n=x_0$。

反过来设 E 中存在序列 $\{x_n\}$（$x_n\neq x_0$，当 $n\neq m$ 时，$x_n\neq x_m$），使得 $\lim\limits_{n\to\infty}x_n=x_0$。

(α,β) 是包含 x_0 的开区间，那么 $\alpha<x_0<\beta$，取 $\varepsilon<\min(x_0-\alpha,\beta-x_0)$，就有

$$\alpha<x_0-\varepsilon<x_0<x_0+\varepsilon<\beta$$

对此 ε，按照 $\lim\limits_{n\to\infty}x_n=x_0$ 的定义，存在一个 N 使得当 $n>N$ 时就有 $|x_n-x_0|<\varepsilon$，或者

$$\alpha<x_0-\varepsilon<x_n<x_0+\varepsilon<\beta$$

这就说明 (α,β) 中含有 E 的异于 x_0 的点，因此 x_0 是 E 的极限点。

定理 4.6.5（波查诺 – 维尔斯特拉斯）

(1) 有界无限集合 E 至少有一个极限点（但此极限点不一定属于 E）；

(2) 任一有界序列 $x_1,x_2,\cdots x_n,\cdots$ 中必存在收敛的子序列

$$x_{n_1},x_{n_2},\cdots,x_{n_k},\cdots,n_1<n_2<n_3<\cdots$$

证明 (1) 由于 E 有界，因此存在闭区间 $[a,b]$ 包含 E。设 $c=\frac{a+b}{2}$，那么在闭区间 $[a,c]$ 和 $[c,b]$ 之中必有一个包含 E 的无限个点，否则 E 将成为有

限集合。设此闭区间是$[a_1,b_1]$。再设 $c_1=\frac{a_1+b_1}{2}$，那么在闭区间$[a_1,c_1]$和$[c_1,b_1]$之中又必有一个包含 E 的无限个点，设此闭区间是$[a_2,b_2]$。如此反复进行，就得到一系列闭区间

$$\cdots[a_n,b_n]\subset\cdots\subset[a_2,b_2]\subset[a_1,b_1]\subset[a,b]$$

其中每一个闭区间都含有 E 中无限个点。且

$$b_n-a_n=\frac{b-a}{2^n}$$

由于$(b_n-a_n)\to 0$，因此根据区间套性质，必存在一个点或实数 x_0 属于所有的闭区间$[a_n,b_n]$，且$\lim\limits_{n\to\infty}b_n=\lim\limits_{n\to\infty}a_n=x_0$。

设(α,β)是包含 x_0 的任一开区间，那么当 n 充分大时，必有$[a_n,b_n]\subset(\alpha,\beta)$，所以$(\alpha,\beta)$含有 E 中无限个点，故 x_0 是 E 的极限点。

(2) 将 $x_1,x_2,\cdots,x_n,\cdots$ 中的数看成点，如果序列$\{x_n\}$所表示的点集是有限集，那么必有点 ξ 在序列$\{x_n\}$中出现无限次，即存在 $n_1<n_2<n_3<\cdots$ 使得

$$x_{n_1}=x_{n_2}=\cdots=x_{n_k}=\cdots=\xi$$

这样$\{x_{n_k}\}$就是我们所需要的子序列。

如果序列$\{x_n\}$所表示的点集 E 是无限集，那么按照(1)中已证的结论，E 有极限点。那么根据定理 4.5.6，E 中包含一个序列$\{x_{n_k}\}$($x_{n_k}\neq x_0$，当 $k_1\neq k_2$ 时，$x_{n_{k_1}}\neq x_{n_{k_2}}$)，使得$\lim\limits_{k\to\infty}x_{n_k}=x_0$(因为 E 本身就是一个序列，所以 E 中包含的序列就是原序列的子序列了)。这就证明了(2)。

注意，上面定理中的“有界”这一条件不能缺少。例如，设 $E=N$ 是全体自然数，那么虽然 E 是无限集，但是 E 没有极限点。

定义 4.6.4 设 E 为一点集，那么

(1) E 的所有极限点所组成的集合称为 E 的导出集，记为 E'；

(2) 如果 $E'\subset E$，则称 E 为闭集；

(3) 如果 $E\subset E'$，则称 E 为己密集；

(4) 如果 $E=E'$，则称 E 为完备集；

(5) 点集 $E\cup E'$ 称为 E 的闭包，记为 $\overline{E}$。

由上面的定义可知，闭集就是含有它的所有极限点的集合，己密集是不含孤立点的集合，完备集是既闭又己密的集合。例如

(1) $E=\left\{1,\frac{1}{2},\frac{1}{3},\cdots,\frac{1}{n},\cdots\right\}$，那么 $E'=\{0\}$，E 既不是闭集也不是己密集；

(2) $E=(a,b)$，那么 $E'=[a,b]$，E 为己密集但不是闭集；

(3) $E=[a,b]$，那么 $E'=[a,b]$，E 为完备集；

(4) $E = \mathbf{R}$(全体实数)，那么 $E' = \mathbf{R}$，所以全体实数构成一个完备集；

(5) $E = \left\{1, \frac{1}{2}, \frac{1}{3}, \cdots, \frac{1}{n}, \cdots, 0\right\}$，那么 $E' = \{0\}$，E 是闭的，但不是已密的；

(6) $E = Q$(全体有理数)，那么 $E' = \mathbf{R}$，E 为已密集但不是闭集；

(7) $E = \varnothing$，那么 $E' = \varnothing$，因此空集是完备集；

(8) E 为有限集，那么 $E' = \varnothing$。故一切有限集是闭的，但不是已密的。

下面是一些有关闭集的定理。

定理 4.6.6　任何集 E 的导出集 E' 是闭集。

证明　如果 E' 是有限集，则由上面例中的(8)可知 E' 是闭集。如果 E' 是无限集，则设 x_0 为 E' 的一个极限点。任取一个包含 x_0 的开区间 (α, β)。由极限点的定义，(α, β) 中必含有 E' 中的点 z，也就是 E 的极限点，根据定理 4.6.4，(α, β) 中必含有 E 的无限个不同的点；同样根据定理4.6.4可知 x_0 是 E 的极限点，这就说明 $x_0 \in E'$，由 x_0 的任意性，即得 $E'' \in E'$。这就说明 E' 是闭集。

定理 4.6.7

(1) 如果 $A \subset B$，则 $A' \subset B'$；

(2) $(A \cup B)' = A' \cup B'$。

证明　(1) 显然；

(2) 由 $A \subset A \cup B$，$B \subset A \cup B$ 及(1)得出 $A' \subset (A \cup B)'$，$B' \subset (A \cup B)'$，因此

$$A' \cup B' \subset (A \cup B)'$$

另一方面，设 $x_0 \in (A \cup B)'$，则在 $A \cup B$ 中存在序列 $\{x_n\}$($x_n \neq x_0$，当 $n \neq m$ 时，$x_n \neq x_m$)，使得 $\lim\limits_{n \to \infty} x_n = x_0$。如果序列 $\{x_n\}$ 中有无限个点属于 A，则 x_0 是 A 的极限点，从而 $x_0 \in A' \subset A' \cup B'$；如果序列 $\{x_n\}$ 中只有有限个点属于 A，那么序列 $\{x_n\}$ 中有无限个点属于 B，即 x_0 是 B 的极限点，从而 $x_0 \in B' \subset A' \cup B'$。因此无论出现哪种情况都成立 $x_0 \in A' \cup B'$，由 x_0 的任意性即得 $(A \cup B)' \subset A' \cup B'$，联合已证的 $A' \cup B' \subset (A \cup B)'$ 即得(2)。

定理 4.6.8

(1) 任何集 E 的闭包 $\overline{E}$ 为闭集；

(2) E 为闭集的充分必要条件是 $E = \overline{E}$。

证明　(1) 事实上我们有

$$(\overline{E})' = (E \cup E')' = E' \cup E'' \subset E' \cup E' = E' \subset \overline{E}$$

(2) 设 $E = \overline{E}$，则由(1) $E' = (\overline{E})' \subset \overline{E} = E$，因此 E 是闭集；反之，如果 E 是闭集，则由 $\overline{E} = E \cup E' \subset E \subset \overline{E}$ 得出 $E = \overline{E}$。

定理 4.6.9　有限个闭集的合集是闭集。

证明　设 F_1, F_2 为两个闭集，则由定理 4.6.7 和闭集的定义得出

$$(F_1 \cup F_2)' = F'_1 \cup F'_2 \subset F_1 \cup F_2$$

这就说明 $F_1 \cup F_2$ 是闭集，依此类推即可得出定理。

注意无限个闭集的合集可能不是闭集。

例如，取 $F_n = \left[\frac{1}{n}, 1\right] (n = 1,2,3,\cdots)$，则每一个 F_n 显然是闭集，但是其和集

$$\bigcup_{n=1}^{\infty} F_n = (0,1]$$

不是闭集。

定理 4.6.10　任意个闭集的交集是闭集。

证明　设 $F = \bigcap_{\xi} F_{\xi}$，其中 F_{ξ} 都是闭集。

由于 $F \subset F_{\xi}$，所以 $F' \subset F'_{\xi}$，而由于 F_{ξ} 都是闭集，因此 $F_{\xi} = F'_{\xi}$，由此式和 $F' \subset F'_{\xi}$ 就得出 $F' \subset F_{\xi}$，因而 $F' \subset \bigcap_{\xi} F_{\xi} = F$，这就说明 F 是闭集。

根据上面的定理可以得出闭集的一个性质如下：

定理 4.6.11　设 F 为闭集，$x_1, x_2, \cdots, x_n, \cdots$ 是 F 中的一个点列，那么如果当 $n \to \infty$ 时，$x_n \to x_0$，则 $x_0 \in F$。

证明　如果点列 $x_1, x_2, \cdots, x_n, \cdots$ 包含无穷个点，那么 x_0 就是 F 的极限点，因而由 F 是闭集的假设就得出 $x_0 \in F$。如果 $x_1, x_2, \cdots, x_n, \cdots$ 只包含有限个不同的点，那么此点列从某一项之后就全都由 x_0 所组成，因此也有 $x_0 \in F$。

下面证明一个非常重要的定理：

波莱尔（Borel, Émile, 1871—1956），法国数学家，生于法国阿韦龙的圣阿夫里克，卒于巴黎。

定理 4.6.12（波莱尔有限覆盖定理）　如果有界闭集 F 被无限个开区间的集合 $\sum$ 所覆盖，那么必可从 $\sum$ 中选取有限个开区间所组成的集合 $\sum^*$ 也覆盖 F。

证明　用反证法证明。假设不存在所说的集合 $\sum^*$，那么 F 必为无限集。由于 F 有界，因此可设 $F \subset [a,b]$。令 $c = \frac{a+b}{2}$，那么 $F \cap [a,c]$ 和 $F \cap [c,b]$ 之中至少有一个不能被 $\sum$ 中有限个开区间所覆盖，把此集合记为 $F \cap [a_1, b_1]$，显然 $F \cap [a_1, b_1]$ 仍是无限集。再令 $c_1 = \frac{a_1+b_1}{2}$，那么 $F \cap [a_1, c_1]$ 和 $F \cap [c_1, b_1]$ 之中至少有一个不能被 $\sum$ 中有限个开区间所覆盖，把此集合记为 $F \cap [a_2, b_2]$，依次类推，将此手续进行下去，我们就得到一个区间套

$$[a,b] \supset [a_1,b_1] \supset [a_2,b_2] \supset \cdots$$

使得 $F \cap [a_n, b_n] (n = 1,2,3,\cdots)$ 不能被 $\sum$ 中有限个开区间所覆盖，且都是无限集。

由于当 $n\to\infty$ 时闭区间 $[a_n,b_n]$ 的长度为 $\frac{b-a}{2^n}\to 0$，因此由区间套性质可知所有的 $[a_n,b_n]$ 有一个公共点 x_0，且 $\lim\limits_{n\to\infty}a_n=\lim\limits_{n\to\infty}b_n=x_0$。

我们证明 x_0 必属于 F。为此首先从 $F\cap[a_1,b_1]$ 中选取一点 x_1，然后再从 $F\cap[a_2,b_2]$ 中选取一个不同于 x_1 的点 x_2（由于 $F\cap[a_2,b_2]$ 是无限集，所以肯定可以选到所需的点）。再从 $F\cap[a_3,b_3]$ 中选取一个不同于 x_1 和 x_2 的点 x_3，如此进行下去，就得到一个 F 中的叙列 $x_1,x_2,\cdots,x_n,\cdots$，由于 $a_n\leqslant x_n\leqslant b_n$，故由两边夹定理可知当 $n\to\infty$ 时，$x_n\to x_0$，因而 x_0 是 F 的极限点，而由于 F 是闭集，这就得出 $x_0\in F$。

由于 $\sum$ 覆盖 F，因此 $\sum$ 中必存在一个开区间 $\sigma_0\in\sum$ 使得 σ_0 覆盖 x_0，但是当 n 充分大时，必有 $[a_n,b_n]\subset\sigma_0$，因而 $F\cap[a_n,b_n]\subset\sigma_0$。这就表示 $F\cap[a_n,b_n]$ 被 $\sum$ 中的一个开区间所覆盖了，而这与 $F\cap[a_n,b_n]$ $(n=1,2,3,\cdots)$ 不能被 $\sum$ 中有限个开区间所覆盖的性质相矛盾。所得的矛盾就说明必存在有限个开区间所组成的集合 $\sum^*$ 也覆盖 F。

注意：这个定理中的有界和闭这两个条件都不可缺少。例如，设 N 是全体自然数所成的集合，则由于 $N'=\varnothing$，因此 N 是一个闭集，对 N 中每一个点 n，开区间 $\left(n-\frac{1}{3},n+\frac{1}{3}\right)$ 显然可以覆盖点 n，因此开区间的集合 $\sum=\left\{\left(n-\frac{1}{3},n+\frac{1}{3}\right)\right\}$ 可以覆盖 N，但是 $\sum$ 的任何有限子集不能覆盖 N，这就说明有界的条件是不可缺少的。

又例如，设 $E=\left\{1,\frac{1}{2},\frac{1}{3},\cdots\right\}$，则 E 是有界的，但不是闭的。对每一个 $\frac{1}{n}$ 取一个小的开区间 σ_n，使得 σ_n 包含 $\frac{1}{n}$，但不包含 E 中其他的点。于是由开区间 $\sigma_n(n=1,2,3,\cdots)$ 组成的集合 $\sum$ 覆盖 E，但是 $\sum$ 的任何有限子集不能覆盖 E。这就说明闭的条件是不可缺少的。

定义 4.6.5（波查诺－维尔斯特拉斯） 和定理 4.6.12（波莱尔有限覆盖定理）是两个非常有力的定理，如同两把大刀，几乎可以解决任何困难，当你没有办法之时，往往是一个可以一试的最后法门。就好像它们本身已经吸收了证明中的基本困难点，它们可以使许多困难定理的证明简化。

现在，就让我们来应用一下这两个定理。

在前面，我们已经给出了几个叙列极限存在的判据，然而这些判据都需对叙列外加一些条件，而一个叙列是否收敛应该是一个由它本身的性质决定的问题，因此自然要提出这样的问题，即是否能由叙列本身的性质来判断它是否收敛？回答是肯定的。对此我们有

定理4.6.13(波查诺－柯西收敛原理)　叙列 $x_1,x_2,\cdots,x_n,\cdots$ 存在有穷极限的充分必要条件是对任意正数 $\varepsilon>0$,存在正整数 N,使得当 $m>N,n>N$ 时就有 $|x_m-x_n|<\varepsilon$。

证明　(1) 设当 $n\to\infty$ 时,叙列$\{x_n\}$存在极限 a,则任给 $\varepsilon>0$,对于正数 $\frac{\varepsilon}{2}>0$,就必存在正整数 N,使得当 $n>N$ 时就有 $|x_n-a|<\frac{\varepsilon}{2}$。

设 $m>N,n>N$,于是就有

$$|x_m-x_n|=|x_m-a+a-x_n|\leqslant|x_m-a|+|x_n-a|<\frac{\varepsilon}{2}+\frac{\varepsilon}{2}\leqslant\varepsilon$$

这就证明了必要性。

(2) 设对任意正数 $\varepsilon>0$,存在正整数 N,使得当 $m>N,n>N$ 时就有 $|x_m-x_n|<\varepsilon$。

那么当 $n>N$ 时,$|x_n-x_{N+1}|<\varepsilon$,于是 $|x_n|<|x_{N+1}|+\varepsilon$,令 $M=\max(|x_1|,|x_2|,\cdots,|x_N|,|x_{N+1}|+\varepsilon)$,那么对一切 n 就都成立 $|x_n|<M$,因此$\{x_n\}$是有界的。

根据定理4.6.5(波查诺－维尔斯特拉斯)由$\{x_n\}$的有界性就得出,$\{x_n\}$必存在收敛到某个极限 a 的子叙列 x_{n_k},使得当 $n\to\infty$ 时 $x_{n_k}\to a$。故根据极限的定义,对任意正数 $\varepsilon>0$,可选取充分大的 k,使得 $|x_{n_k}-a|<\frac{\varepsilon}{2}$,$n_k>N$。又根据我们的假设,对 $\varepsilon>0$,又存在着正整数 N,使得当 $n_k>N,n>N$ 时就有 $|x_n-x_{n_k}|<\frac{\varepsilon}{2}$,因而当 $n>N$ 时就有

$$|x_n-a|=|x_n-x_{n_k}+x_{n_k}-a|\leqslant|x_n-x_{n_k}|+|x_{n_k}-a|<\frac{\varepsilon}{2}+\frac{\varepsilon}{2}\leqslant\varepsilon$$

而这就是说当 $n\to\infty$ 时 $x_n\to a$,因而充分性得证。

这个定理的充分性假如不用定理4.6.5,简直就没有什么办法。

上面说了一些极限的性质和存在性的判据。在所有的极限中,趋于零的叙列和函数是一种比较特殊也是最基本的极限过程。所以下面我们特别来讨论一下和这种过程有关的一些概念。

定义4.6.6　如果 $\lim\limits_{x\to x_0}f(x)=0$,也即如果对任意 $\varepsilon>0$,存在 $\delta>0$ 使得当 $|x-x_0|<\delta$ 时就有 $|f(x)|<\varepsilon$,则称当 $x\to x_0$ 时 $f(x)$ 是无穷小量,记为当 $x\to x_0$ 时 $f(x)=o(1)$;特别,如果 $\lim\limits_{n\to\infty}a_n=0$,那么当 $n\to\infty$ 时,$a_n=o(1)$。

下面是一些常见的无穷小量:当 $x\to0$ 时,$x,\sin x,\ln(1+x),e^x-1$ 都是无穷小量。当 $n\to\infty$ 时,$\frac{1}{n},\frac{1}{\sqrt{n}},\frac{1}{n^2}$ 等也都是无穷小量。

与无穷小量相反的概念是无穷大量。

定义 4.6.7 如果$\lim\limits_{x \to x_0} |f(x)| = \infty$，也即如果对任意 $M > 0$，存在 $\delta > 0$ 使得当 $|x - x_0| < \delta$ 时就有 $|f(x)| > M$，则称当 $x \to x_0$ 时 $f(x)$ 是无穷大量；特别，如果 $\lim\limits_{n \to \infty} |a_n| = \infty$，那么当 $n \to \infty$ 时，a_n 是无穷大量。

例如当 $x \to \infty$ 时，$x^{\alpha}(\alpha > 0)$，e^x，$\ln x$ 都是无穷大量。

无穷大量和无穷小量的概念，只是对趋于无穷大和趋于零的过程起了一个名称，但是在具体问题中，我们更关心的却是各种不同的无穷大和无穷小之间的关系，它们变化的相对的快慢，为此，我们还需引进"阶"的概念。

定义 4.6.8 如果$\lim\limits_{x \to x_0} \dfrac{f(x)}{g(x)} = 0$，则称当 $x \to x_0$ 时，$f(x)$ 是相对于 $g(x)$ 的无穷小量，记为当 $x \to x_0$ 时，$f(x) = o(g(x))$。

如果 $f(x)$ 和 $g(x)$ 都是无穷小量，则称 $f(x)$ 是比 $g(x)$ 高阶的无穷小量。

如果 $f(x)$ 和 $g(x)$ 都是无穷大量，则称 $f(x)$ 是比 $g(x)$ 低阶的无穷大量。

我们还需引进所谓"等价的无穷小"和"等价的无穷大"概念以及大 O 的概念才能使我们的讨论完全。

定义 4.6.9 如果$\lim\limits_{x \to x_0} \dfrac{f(x)}{g(x)} = 1$，则称当 $x \to x_0$ 时，$f(x)$ 与 $g(x)$ 是等价的，记为当 $x \to x_0$ 时，$f(x) \sim g(x)$。

例如可以证明当 $x \to 0$ 时 $\sin x \sim x$，$e^x - 1 \sim x$。

定义 4.6.10 设 $g(x) > 0$，如果存在常数 $C > 0$，使得在开区间 (a, b) 上

$$|f(x)| \leqslant Cg(x)$$

则称 $g(x)$ 是 $f(x)$ 的强函数，记为

$$f(x) = O(g(x)), x \in (a, b)$$

例如可以证明

$$\cos x = O(1), \ln x = O(x), x > 1$$

大 O 和小 o 有以下性质：

定理 4.6.14

(1) 如果 $f(x)$ 是无穷大量，而当 $x \to x_0$ 时，$\varphi(x) = O(1)$，则当 $x \to x_0$ 时，$\varphi(x) = o(f(x))$；

(2) 如果 $f(x) = O(\varphi)$，$\varphi = O(\psi)$，则 $f(x) = O(\psi)$；

(3) 如果 $f(x) = O(\varphi)$，$\varphi = o(\psi)$，则 $f(x) = o(\psi)$；

(4) $O(f) + O(g) = O(f + g)$；

(5) $O(f) + o(f) = O(f)$；

(6) $o(f) + o(g) = o(|f| + |g|)$；

(7) $O(f) \cdot O(g) = O(f \cdot g)$；

(8) $o(1) \cdot O(f) = o(f)$；

(9) $O(1)\cdot o(f)=o(f)$;

(10) $o(f)\cdot o(g)=o(f\cdot g)$;

(11) $(O(f))^k=O_k(f^k)$，k 是自然数，O_k 表示大 O 中的常数与 k 有关；

(12) $(o(f))^k=o(f^k)$;

(13) 如果 $f\sim g$，$g\sim h$，则 $f\sim h$；

(14) 如果 $f\sim g$，$h=0(g)$，则 $f\sim g\pm h$。

这些性质都很容易验证，请读者自己作为练习。

例 4.6.2 求极限 $\lim\limits_{n\to\infty}\cos^n\dfrac{x}{\sqrt{n}}$。

解 容易证明 $\cos x=1-\dfrac{x^2}{2}+o(x^4)$，因此

$$\left(\cos\frac{x}{\sqrt{n}}\right)^n=\left(1-\frac{x^2}{2n}+o\left(\frac{1}{n^2}\right)\right)^n=e^{n\ln\left(1-\frac{x^2}{2n}+o\left(\frac{1}{n^2}\right)\right)}=e^{n\left(-\frac{x^2}{2n}+o\left(\frac{1}{n^2}\right)\right)}=$$

$$e^{-\frac{x^2}{2}\left(1+o\left(\frac{1}{n}\right)\right)}=e^{-\frac{x^2}{2}}\left(1+o\left(\frac{1}{n}\right)\right)$$

这就证明了

$$\lim_{n\to\infty}\cos^n\frac{x}{\sqrt{n}}=e^{-\frac{x^2}{2}}$$

例 4.6.3 $\lim\limits_{n\to\infty}n^2(\sqrt[n]{x}-\sqrt[n+1]{x})$。

解 易证 $e^x=1+x+o(x^2)$，因此

$$n^2(\sqrt[n]{x}-\sqrt[n+1]{x})=n^2x^{\frac{1}{n}}(1-x^{-\frac{1}{n(n+1)}})=n^2x^{\frac{1}{n}}(1-e^{-\frac{1}{n(n+1)}\ln x})=$$

$$n^2x^{\frac{1}{n}}\left(1-\left(1-\frac{1}{n(n+1)}\ln x+o\left(\frac{1}{n^4}\right)\right)\right)=$$

$$n^2x^{\frac{1}{n}}\left(\frac{\ln x}{n(n+1)}+o\left(\frac{1}{n^4}\right)\right)=x^{\frac{1}{n}}\ln x+o\left(\frac{1}{n^2}\right)$$

这就证明了

$$\lim_{n\to\infty}n^2(\sqrt[n]{x}-\sqrt[n+1]{x})=\ln x$$

例 4.6.4 设 $x_0>0$，$x_{n+1}=\ln(1+x_n)$，证明：x_n 是一个无穷小量，并求出它的幂函数形式的等价无穷小。

解 (1) $x_0>0$，$0<x_{n+1}=\ln(1+x_n)<x_n$，因此 x_n 是单调递减有下界的叙列，因而是收敛的。因此可设 $\lim\limits_{n\to\infty}x_n=x$，在 $x_{n+1}=\ln(1+x_n)$ 的两边令 $n\to\infty$ 就得到 $x=\ln(1+x)$，这个方程在 $x=0$ 的邻域中有唯一解 $x=0$，因此就证明了 $\lim\limits_{n\to\infty}x_n=0$，即 x_n 是一个无穷小量。

(2) 假设当 $n\to\infty$ 时，$x_n\sim cn^a$，那么把这一关系式代入 $x_{n+1}=\ln(1+x_n)$ 后就得到

$$c(n+1)^{\alpha} = \ln(1+cn^{\alpha}) = cn^{\alpha} - \frac{1}{2}c^2 n^{2\alpha} + o(n^{2\alpha})$$

$$\left(1+\frac{1}{n}\right)^{\alpha} = 1 - \frac{1}{2}cn^{\alpha} + o(n^{\alpha})$$

$$1 + \frac{\alpha}{n} + o\left(\frac{1}{n}\right) = 1 - \frac{1}{2}cn^{\alpha} + o(n^{\alpha})$$

比较上式两边的同类项，就可得到 $\alpha = -1, c = 2$。

不过要注意，上边所写的并不能算是严格的证明，只能算是一种思考的过程，但是这一过程正是做研究工作时的真实情况。这种思考问题的方法（当然还有许多其他的思考方法，这只是其中一种）是当我们遇到一个问题，还不知道如何解决时，先假定我们的猜想是成立的（在这里就是假定当 $n \to \infty$ 时，$x_n \sim cn^{\alpha}$），然后看看是否能得出一些性质和推论，当我们得出了足够的性质后，再看看问题是否在具有这些性质的情况下能够得到解决。下面我们就来严格地证明当 $n \to \infty$ 时，$x_n \sim \dfrac{2}{n}$。

(3) 易于证明当 x 充分小时，成立

$$x - \frac{x^2}{2} < \ln(1+x) < x - \left(\frac{1}{2} - \epsilon\right)x^2 \qquad ①$$

$$1 + x < \frac{1}{1-x} < 1 + (1+\epsilon)x \qquad ②$$

从 ① 得出

$$x_n - \frac{x_n^2}{2} < x_{n+1} = \ln(1+x_n) < x_n - \left(\frac{1}{2} - \epsilon\right)x_n^2$$

由上式和式 ② 再得出

$$\frac{1}{x_n} + \frac{1}{2} - \epsilon \leqslant \frac{1 + \left(\frac{1}{2} - \epsilon\right)x_n}{x_n} <$$

$$\frac{1}{x_n\left(1 + \left(\frac{1}{2} - \epsilon\right)x_n\right)} < \frac{1}{x_{n+1}} < \frac{1}{x_n\left(1 - \frac{1}{2}x_n\right)} <$$

$$\frac{1 + (1+\epsilon)\frac{1}{2}x_n}{x_n} < \frac{1}{x_n} + \frac{1+\epsilon}{2}$$

反复应用上式就得出

$$\frac{1}{x_N} + k\left(\frac{1}{2} - \epsilon\right) < \frac{1}{x_{N+k}} < \frac{1}{x_N} + k\frac{1+\epsilon}{2}$$

$$\frac{1}{(N+k)x_N} + \frac{k}{N+k}\left(\frac{1}{2} - \epsilon\right) < \frac{1}{(N+k)x_{N+k}} < \frac{1}{(N+k)x_N} + \frac{k}{N+k}\frac{1+\epsilon}{2}$$

或当 $n > N$ 时

$$\frac{1}{nx_N}+\frac{n-N}{n}\left(\frac{1}{2}-\epsilon\right)<\frac{1}{nx_n}<\frac{1}{nx_N}+\frac{n-N}{n}\cdot\frac{1+\epsilon}{2}$$

由上式和两边夹定理即得，当 $n\to\infty$ 时，$\lim\limits_{n\to\infty} nx_n$ 存在，因此可设 $\lim\limits_{n\to\infty} nx_n=x$，在上式中令 $n\to\infty$ 就得到

$$\frac{1}{2}-\epsilon\leqslant\frac{1}{x}\leqslant\frac{1+\epsilon}{2}$$

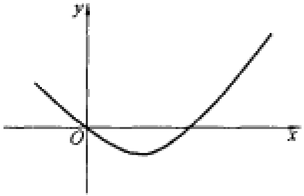
再在上式中令 $\epsilon\to 0$ 就得出 $x=2$。这样，我们一方面得出当 $n\to\infty$ 时，x_n 的阶是 $\frac{2}{n}$，同时也求出了极限 $\lim\limits_{n\to\infty} nx_n=2$。

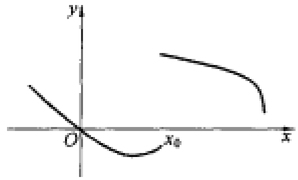
有了阶这个概念之后，光有关阶的内容，我们就有了永远研究不完的问题了。

比如说，在你的工作中，你遇见了某个新的，还未被别人研究过的函数 $f(x)$，并且已知当 $x\to x_0$ 时，$f(x)\to a_1$。那么你马上就可提出一个问题，就是无穷小 $f(x)-a_1$ 的阶是什么？我们把这个问题再提得更加明确些。因为如果泛泛地提这个问题，那你回答 $f(x)-a_1$ 的阶就是 $f(x)-a_1$ 也不能算错，但是这样回答也就等于什么也没有说。所以我们问 $f(x)-a_1$ 的阶是什么的意思是能否找到一个我们所熟悉的函数 $g_1(x)$ 使得 $f(x)-a_1\sim g_1(x)$，如果可能的话，最好能求出 $c(x-x_0)^a$ 形式 $g_1(x)$ 的来；如果你找到了这样的 $g_1(x)$，马上又会发生下一个问题，就是无穷小 $f_1(x)-g_1(x)$ 的阶又是什么？其中 $f_1(x)=f(x)-a_1$，如此不断继续下去，就形成了一个越来越困难的问题链。

请你绝对不要以为这是数学家们没事干了所提出的没有意义的问题。如果你遇到的的确是一个以前没有人研究过的，其性质还未知的，而对了解实际问题起着非常重要作用甚至是本质作用的函数，那么上述工作就是绝对有意义的，这可以说是了解这一函数的特性的第一步。我可以举出许多科学家的重要工作，他们的第一步工作往往就是研究某个新的函数的上述特性。比如，在常微分方程领域，有一个叫安德罗诺夫的数学家，在他写的两本书《二阶动力系统的定性理论》和《平面系统的的分支理论》中的开始部分的最重要的工作就是研究一个被称为"后继函数"$v(u)$，$v(0)=0$ 的无穷小的阶，而且仅仅第一步的结果，也就是给出了 $v(u)$ 的 cu^a 形式的阶，在他的理论中，乃至一直到今天都是一个基本重要的结果，由此结果出发，人们就得出了许多重要的稳定性判据。本书作者之一对后继函数的更高的阶作了研究，并据此给出了临界情况下分解线圈（现称为同宿环）的稳定性判据。（参见冯贝叶，钱敏．鞍点分界线圈的稳定性及其分支出极限环的条件数学学报，1985，28(1)：53-70）。

现在我们来考虑函数的一种重要性质：连续性。说函数 $f(x)$ 是连续的，从直观上来是它的图象不能发生像下图右边图中那种突然跳跃





发生间断时，$f(x)$ 的图象本来从左边过来到点 x_0 之前附近时，$f(x)$ 的值一直是小于 0 的，也就是 $f(x)$ 的图象一直是在 x 轴下方的，可是到了 x_0 处，却突然跳到 x 轴上方去了。显然，如果函数的值老是跳来跳去，就显得很没有规律，因为一是你不知道它什么时候跳，二是在发生间断时，函数值要跳多少也不知道，另外这种突然的跳动也跟我们在日常生活中观察到的大多数规律不符合。因此如果不是由于确实需要，我们自然愿意首先考虑不间断的也即连续的函数。既然间断的特征是函数值要发生跳跃，因此连续的特征就是当自变量 x 接近某个值 x_0 时，函数值 $f(x)$ 也必须接近 $f(x_0)$。由此就可以给出函数连续的定义如下。

定义 4.6.11 任给正数 $\epsilon > 0$，如果存在正数 $\delta > 0$，使得只要 $|x - x_0| < \delta$ 就有 $|f(x) - f(x_0)| < \epsilon$，那么就称函数 $f(x)$ 在点 x_0 是连续的。

如果函数 $f(x)$ 在集合 E 的每一个点都是连续的，就称 $f(x)$ 在 E 上是连续的。

上面函数的连续性定义中的 δ 除了明显地在字面上就依赖于 ϵ 之外，实际上，虽然容易让人忽略，一般的还依赖于 x_0。

例 4.6.5 证明：$\frac{1}{x}$ 在 $(0, \infty)$ 上是连续的。

证明 任取 $x_0 > 0$，首先设 $|x - x_0| < \frac{x_0}{2}$，于是 $x > \frac{x_0}{2}$，因而

$$\left|\frac{1}{x} - \frac{1}{x_0}\right| = \frac{x - x_0}{xx_0} < \frac{2}{x_0^2}|x - x_0|$$

因而只要取

$$|x - x_0| < \min\left(\frac{x_0}{2}, \frac{x_0^2\epsilon}{2}\right)$$

就有

$$\left|\frac{1}{x} - \frac{1}{x_0}\right| < \epsilon$$

由于 $x_0 > 0$ 的任意性，这就证明了 $\frac{1}{x}$ 在 $(0, \infty)$ 上是连续的。

这里的 $\delta = \min\left(\frac{x_0}{2}, \frac{x_0^2\epsilon}{2}\right)$ 就明显地既依赖于 ϵ 也依赖于 x_0，它的表达式表明，在 ϵ 相同的情况下，x_0 越大，δ 就允许取得越大，而如果 $x_0 \to 0$，则 δ 也必须

$\to 0$。

受此启发，就从连续的概念里又抽出下面的概念：

定义 4.6.12 如果对于任意 $\epsilon > 0$，能够求出正数 $\delta > 0$，使得对于集合 E 中任意的两点 x_1, x_2，只要 $|x_1 - x_2| < \delta$ 就有 $|f(x_1) - f(x_2)| < \epsilon$，那么就称函数 $f(x)$ 在 E 中是一致连续的。

一致连续的概念和连续概念的区别在于它是一个整体的性质，而在一点连续却是一个局部的性质。一个在某个区间上连续的函数不一定是一致连续的，例如，例 4.6.2 中的函数 $\frac{1}{x}$ 在 $(0, \infty)$ 上是连续的，却不是在 $(0, \infty)$ 上一致连续的。

然而如果你举出足够的不是一致连续的函数的例子，你就会发现，它们都不是定义在一个闭区间上的函数，这不是一个偶然的现象，事实上，在闭区间上定义的连续函数不可能发生上述现象，这就是

定理 4.6.15（康托尔定理） 在闭区间 $[a, b]$ 上连续的函数必定是一致连续的。

康托尔（Cantor, Georg Ferdinand Ludwig philipp, 1845—1918），德国数学家，集合论的创始人。

证明 设函数 $f(x)$ 是在闭区间 $[a, b]$ 上连续的函数。那么任给正数 $\epsilon > 0$，对于 $\frac{\epsilon}{2} > 0$ 和 $[a, b]$ 中的点 x_0，根据 $f(x)$ 的连续性，可以求出正数 $\delta > 0$，使得只要 $|x - x_0| < \delta$ 就有 $|f(x) - f(x_0)| < \frac{\epsilon}{2}$。现在设 x_1, x_2 是开区间 $(x_0 - \delta, x_0 + \delta)$ 中任意的两点，那么就有

$$\begin{aligned}|f(x_1) - f(x_2)| &= |f(x_1) - f(x_0) + f(x_0) - f(x_2)| \leqslant \\ &|f(x_1) - f(x_0)| + |f(x_2) - f(x_0)| < \\ &\frac{\epsilon}{2} + \frac{\epsilon}{2} < \epsilon\end{aligned}$$

因而，开区间 $\sigma(x_0) = (x_0 - \delta(x_0), x_0 + \delta(x_0))$ 具有性质：任意两点 x', x'' 只要都属于开区间 $\sigma(x_0)$ 就成立 $|f(x_1) - f(x_2)| < \epsilon$。

对闭区间 $[a, b]$ 中每一点 x_0，显然开区间 $\overline{\sigma}(x_0) = \left(x_0 - \frac{\delta(x_0)}{2}, x_0 + \frac{\delta(x_0)}{2}\right)$ 覆盖了点 x_0，因而由这些开区间组成的集合 $\overline{\sum} = \left\{\left(x_0 - \frac{\delta(x_0)}{2}, x_0 + \frac{\delta(x_0)}{2}\right)\right\}, x_0 \in [a, b]$ 就覆盖了闭区间 $[a, b]$。

根据定理 4.6.12，从 $\overline{\sum}$ 中定可选出有限个开区间 $\overline{\sigma}_1, \overline{\sigma}_2, \cdots, \overline{\sigma}_n$ 组成的集合 $\sum^*$ 也可覆盖闭区间 $[a, b]$，其中 $\overline{\sigma}_i$ 具有形式 $\overline{\sigma}_i = \left(x_i - \frac{\delta_i}{2}, x_i + \frac{\delta_i}{2}\right)$。现在设 $\delta^* = \min\left(\frac{\delta_1}{2}, \frac{\delta_2}{2}, \cdots, \frac{\delta_n}{2}\right)$，并设 x', x'' 是满足关系式 $|x' - x''| < \delta^*$ 的任意

两点。那么由于$\sum^*$覆盖了闭区间$[a,b]$，因此x'必定要属于某一个开区间$\bar{\sigma}_k=\left(x_k-\frac{\delta_k}{2},x_k+\frac{\delta_k}{2}\right)$，因而当然也属于开区间$\sigma_k=(x_k-\delta_k,x_k+\delta_k)$。由于

$$\begin{aligned}|x''-x_k|=|x''-x'+x'-x_k|\leqslant\\ |x''-x'|+|x'-x_k|<\\ \delta^*+\frac{\delta_k}{2}\leqslant\frac{\delta_k}{2}+\frac{\delta_k}{2}\leqslant\delta_k\end{aligned}$$

这就说明x''和x'都属于开区间$\sigma_k=(x_k-\delta_k,x_k+\delta_k)$，因而根据开区间$\sigma_k=(x_k-\delta_k,x_k+\delta_k)$的性质就得知$|f(x_1)-f(x_2)|<\epsilon$。由于$\delta^*$完全不依赖于$x',x''$的选取，因此这就证明了$f(x)$在闭区间$[a,b]$是一致连续的。

习题 4.6

1. 设X,Y是直线上的点集，f是$X\to Y$的连续映射。证明：

(1) Y中每个开集V在f下的逆象$f^{-1}(V)=\{x\in X\mid f(x)\in V\}$是$X$中的开集；

(2) Y中每个闭集F在f下的逆象$f^{-1}(F)=\{x\in X\mid f(x)\in F\}$是$X$中的闭集；

(3) 对任何$A\subset X$，$f(\overline{A})\subset\overline{f(A)}$。

2. 设$f:X\to\mathbf{R}$是连续函数，证明：

(1) $\{x\mid f(x)>c\}$和$\{x\mid f(x)<c\}$都是开集；

(2) $x\mid f(x)\geqslant c\}$和$\{x\mid f(x)\leqslant c\}$都是闭集。

3. 证明$f:X\to\mathbf{R}$是连续函数的充分必要条件是：

(1) 对任何$c\in\mathbf{R}$，$\{x\mid f(x)>c\}$和$\{x\mid f(x)<c\}$都是X的开集；或者

(2) 对任何$c\in\mathbf{R}$，$\{x\mid f(x)\geqslant c\}$和$\{x\mid f(x)\leqslant c\}$都$X$的是闭集。

4. 举例说明仅有3(1)的一半条件：对任何$c\in\mathbf{R}$，$\{x\mid f(x)>c\}$都是X的开集不能保证$f:X\to\mathbf{R}$是连续函数。

5. 证明：$f(x)=\frac{1}{x}$在开区间$(0,1)$上不是一致连续的。

6. 设函数$f(x)$定义在$[a,b]$上，如果存在一个正数$M>0$，使得对任意$x,y\in[a,b]$都有$|f(x)-f(y)|\leqslant M|x-y|$，则称$f(x)$是在$[a,b]$上李普希茨(Lipschitz)连续的。

证明：在任何包含0的闭区间上，$f(x)=x^2$是李普希茨连续的，但是$\sqrt{|x|}$不是。

7. 设$f(x)$在$[a,\infty)$上连续，当$x\to\infty$时，$f(f(x))\to\infty$，证明：当$x\to\infty$时，$f(x)\to\infty$。

8. 设叙列 x_n 具有性质：$|x_m - x_n| \leqslant \max\{|x_m - x_{m-1}|, |x_n - x_{n-1}|\}$（$m, n \geqslant 2$）。证明：$x_n$ 是有界的。

9. 有界叙列 $\{x_n\}$ 的最小的聚点称为叙列 $\{x_n\}$ 的下极限，记为 $\underline{\lim}_{n\to\infty} x_n$；最大的聚点称为叙列 $\{x_n\}$ 的上极限，记为 $\overline{\lim}_{n\to\infty} x_n$，证明：

(1) $\lim_{n\to\infty} x_n$ 存在的充分必要条件是 $\underline{\lim}_{n\to\infty} x_n = \overline{\lim}_{n\to\infty} x_n$；

(2) $\underline{\lim}_{n\to\infty} x_n + \underline{\lim}_{n\to\infty} y_n \leqslant \underline{\lim}_{n\to\infty} (x_n + y_n) \leqslant \underline{\lim}_{n\to\infty} x_n + \overline{\lim}_{n\to\infty} y_n$；

(3) $\underline{\lim}_{n\to\infty} x_n + \overline{\lim}_{n\to\infty} y_n \leqslant \overline{\lim}_{n\to\infty} (x_n + y_n) \leqslant \overline{\lim}_{n\to\infty} x_n + \overline{\lim}_{n\to\infty} y_n$。

10. 设 $x_n \geqslant 0, y_n \geqslant 0$（$n = 1, 2, \cdots$），证明：

(1) $\underline{\lim}_{n\to\infty} x_n \cdot \underline{\lim}_{n\to\infty} y_n \leqslant \underline{\lim}_{n\to\infty} x_n y_n \leqslant \underline{\lim}_{n\to\infty} x_n \cdot \overline{\lim}_{n\to\infty} y_n$；

(2) $\underline{\lim}_{n\to\infty} x_n \cdot \overline{\lim}_{n\to\infty} y_n \leqslant \overline{\lim}_{n\to\infty} x_n y_n \leqslant \overline{\lim}_{n\to\infty} x_n \cdot \overline{\lim}_{n\to\infty} y_n$。

11. 证明：如果 $x_n \geqslant 0$（$n = 1, 2, \cdots$）并且 $\overline{\lim}_{n\to\infty} x_n \cdot \overline{\lim}_{n\to\infty} \frac{1}{x_n} = 1$，则叙列 $\{x_n\}$ 是收敛的。

12. (1) 设存在极限 $\lim_{x\to 0} \frac{f(x)}{x}$，又当 $x \to 0$ 时，$f(x) - f\left(\frac{x}{2}\right) = o(x)$，证明：当 $x \to 0$ 时，$f(x) = o(x)$；

(2) 设当 $x \to 0$ 时，$f(x) \to 0$，$f(x) - f\left(\frac{x}{2}\right) = o(x)$，证明：当 $x \to 0$ 时，$f(x) = o(x)$。

13. 设数列 $\{x_n\}$ 满足条件 $0 \leqslant x_{m+n} \leqslant x_m + x_n$（$m, n = 1, 2, \cdots$）。证明：存在极限 $\lim_{n\to\infty} \frac{x_n}{n}$。

14. (1) 设 $l = \underline{\lim}_{n\to\infty} x_n$，$L = \overline{\lim}_{n\to\infty} x_n$。证明：如果叙列 $\{x_n\}$ 有界，且 $\lim_{n\to\infty}(x_{n+1} - x_n) = 0$，则闭区间 $[l, L]$ 中的任何一个数都是此叙列的聚点。

(2) 设 $f(x)$ 是 $[a, b] \to [a, b]$ 的连续映射，x 是 $[a, b]$ 内任一点，令 $x_1 = x$，$x_{n+1} = f(x_n)$，证明：x_n 收敛的充分必要条件是 $\lim_{n\to\infty}(x_{n+1} - x_n) = 0$。

15. 设 $S_n = a_1 + a_2 + \cdots + a_n$，当 $n \to \infty$ 时，S_n 收敛，$\lim_{n\to\infty} na_n = c$，证明：$c = 0$。

16. 设 $S_n = a_1 + a_2 + \cdots + a_n$，当 $n \to \infty$ 时，S_n 收敛，举例说明 $\lim_{n\to\infty} na_n$ 可以不存在。

17. 设 $S_n = a_1 + a_2 + \cdots a_n$，当 $n \to \infty$ 时，S_n 收敛，a_n 单调递减。证明：$\lim_{n\to\infty} na_n = 0$。

4.7 隔离性和稠密性

下面来考察闭集的更深刻的性质。

首先我们已知道如果 x,y 是数轴上的两点，那么 x,y 之间的距离就是 $|x-y|$，如果记 $\rho(x,y)=|x-y|$，则 $\rho(x,y)$ 具有以下性质：

(1) $\rho(x,y)\geqslant 0$，当且仅当 $x=y$ 时，$\rho(x,y)=0$；

(2) $\rho(x,y)=\rho(y,x)$；

(3) $\rho(x,y)+\rho(y,z)\leqslant\rho(x,z)$。

由此引出下面的概念：

定义 4.7.1 设 X 是一个集合，如果存在一个映射 $\rho:X\times X\to R(x,y)\mapsto\rho(x,y)$ 满足以下性质：

(1) $\rho(x,y)\geqslant 0$，当且仅当 $x=y$ 时，$\rho(x,y)=0$(正定性)；

(2) $\rho(x,y)=\rho(y,x)$(对称性)；

(3) $\rho(x,y)+\rho(y,z)\leqslant\rho(x,z)$(三角形不等式)。

则称(X,ρ)为度量(或距离)空间，ρ 称为 X 上的度量(或距离)，$\rho(x,y)$ 称为点 x 和 y 之间的距离。

现在考虑更进一步的问题：既然点和点之间可以定义距离的概念，那么自然要问，点和集合，乃至集合与集合之间是否也能有距离的概念？回答是肯定的。

定义 4.7.2 设 x_0 为一点，E 为一个非空的点集。则 x_0 与 E 中的点的距离的下确界就称为点 x_0 与点集 E 之间的距离，记为 $\rho(x_0,E)$，$\rho(x_0,E)=\inf\{\rho(x_0,x)\mid\in E\}$。

显然 $\rho(x_0,E)$ 一定存在且 $\rho(x_0,E)\geqslant 0$。如果 $x_0\in E$，则 $\rho(x_0,E)=0$。但是反过来却不一定对。例如如果 $x_0=0,E=(0,1)$，则 $\rho(x_0,E)$，但是 $x_0\notin E$。

定义 4.7.3 设 A 和 B 是两个不空的点集，则 A 和 B 之间的点的距离的下确界就称为 A 和 B 之间的距离，记为 $\rho(A,B)$，$\rho(A,B)=\inf\{\rho(x,y)\mid x\in A,y\in B\}$。

显然 $\rho(A,B)$ 一定存在，且 $\rho(A,B)=\rho(B,A)\geqslant 0$。

如果 A 与 B 有公共点，则 $\rho(A,B)=0$，但是反过来的结论却不一定成立。例如，设 $A=(-1,0)$，$B=(0,1)$，则 $\rho(A,B)=0$，然而 $A\cap B=\varnothing$。

以上说明是针对一般的集合而言，但是如果 A,B 都是闭集，则附加一定条件后，就可得到更加确切的结果如下：

定理 4.7.1 设 A 和 B 都是非空的闭集，且其中至少有一个是有界的，那么

必存在点 $x^* \in A, y^* \in B$ 使得

$$\rho(x^*, y^*) = \rho(A, B)$$

证明 对每一个自然数 n，$\frac{1}{n}$ 是一个正数。根据下确界的定义对于$\frac{1}{n} > 0$ 存在两个点

$$x_n \in A, y_n \in B$$

使得
$$\rho(A, B) \leqslant \rho(x_n, y_n) < \rho(A, B) + \frac{1}{n}$$

由假设可知 A 和 B 之中至少有一个集合是有界的，不妨设 A 有界，因此 $\{x_n\}$ 是有界数列，因而由波查诺 - 维尔斯特拉斯定理知道可从 $\{x_n\}$ 中抽出一个收敛子列 $\{x_{n_k}\}$ 使得当 $k \to \infty$ 时，$n_k \to \infty$，$x_{n_k} \to x^*$。由于 A 是闭集，因此 $x^* \in A$。

由于 $\{x_n\}$ 是有界数列，所以可设 $|x_n| < C$，因而

$$|y_{n_k}| \leqslant |x_{n_k}| + |y_{n_k} - x_{n_k}| < C + \rho(A, B) + \frac{1}{n_k} \leqslant C + \rho(A, B) + 1$$

这说明 $\{y_{n_k}\}$ 也是有界数列。仍由波查诺 - 维尔斯特拉斯定理知道可从 $\{y_{n_k}\}$ 中抽出一个收敛子列 $\{y_{n_{k_i}}\}$ 使得当 $i \to \infty$ 时，$k_i \to \infty$，$n_{k_i} \to \infty$，$y_{n_{k_i}} \to y^*$。由于 B 是闭集，因此 $y^* \in B$。

从子叙列 $\{y_{n_{k_i}}\}$ 的选取方法即知

$$\rho(x^*, y^*) = |y^* - x^*| = \lim_{i \to \infty} |y_{n_{k_i}} - x_{n_{k_i}}| = \rho(A, B)$$

这就证明了定理。

这个定理中的 A, B 之中至少一个集合是有界的条件和 A, B 都是闭集的条件均不可缺少。例如，如果设 $M = \{n\}$，$N = \left\{n + \frac{1}{2n}\right\}$，则由于 $M' = N' = \varnothing$，因此 M, N 都是闭集。显然 $\rho(M, N) = 0$，但是因为 $M \cap N = \varnothing$，$\rho(x^*, y^*) = 0$ 蕴含 $x^* = y^*$。所以不可能存在 x^*, y^* 使得 $x^* \in M, y^* \in N, p(x^*, y^*) = 0$。

再例如，如果设 $A = [1,2)$，$B = [3,5]$，则 $\rho(A, B) = 1$，然而不存 x^*, y^* 在使得 $x^* \in A, y^* \in B, \rho(x^*, y^*) = 1$。

由定理 4.7.1 立刻得出：

定理 4.7.2

(1) 设 A, B 都是闭集且其中至少一个集合是有界的，那么如果 $\rho(A, B) = 0$，则 $A \cap B \neq \varnothing$，即 A, B 必有公共点；

(2) 设 F 是非空的闭集，x_0 是任意一点，则必存在 $x^* \in F$ 使得 $\rho(x_0, x^*) = \rho(x_0, F)$；

(3) 如果点 x_0 和闭集 F 满足条件 $\rho(x_0,F)=0$，则 $x_0\in F$。

为得出闭集的隔离性，我们首先证明以下引理：

引理 4.7.1 设 A 是非空点集，$d>0$，$U=\{x\mid\rho(x,A)<d\}$，则 $A\subset U$，且 U 是开集。

证明 因为 A 中的点 x 都满足条件 $\rho(x,A)=0$，故显然 $A\subset U$。任取 $x_0\in U$，则 $\rho(x_0,U)<d$，从而 A 中必有点 x^* 使得 $\rho(x_0,x^*)<d$，令

$$r=d-\rho(x_0,x^*)>0,V=\{x,\mid\rho(x_0,x)<r\}$$

在 V 中任取一点 y，则 $\rho(x_0,y)<r$，故

$$\rho(x^*,y)\leqslant\rho(y,x_0)+\rho(x_0,x^*)<r+d-r=d$$

因此 $\rho(y,A)<d$，$V\subset U$。这说明 U 具有性质：如果点 $x_0\in U$，那么 x_0 的邻域 $V\subset U$，因此 U 是开集。这就证明了引理。

引理 4.7.2 设 A,B 是两个非空点集，$\rho(A,B)=r>0$。

$$U=\{x\mid\rho(x,A)<\frac{r}{2}\},V=\{x\mid\rho(x,B)<\frac{r}{2}\}$$

则 $U\cap V=\varnothing$。

证明 用反证法，假设 $U\cap V\neq\varnothing$，那么必存在 $z\in U\cap V$，因此

$$\rho(z,A)<\frac{r}{2},\rho(z,B)<\frac{r}{2}$$

由上式又得出必存在点 $x\in A,y\in B$ 使得 $\rho(z,x)<\frac{r}{2},\rho(z,y)<\frac{r}{2}$，因而 $\rho(x,y)<r$，这又说明 $\rho(A,B)<r$，而这与假设矛盾，所得的矛盾就证明了引理。

定理 4.7.3(隔离性) 设 F_1,F_2 是不相交的闭集，则必存在开集 G_1,G_2 使得

$$F_1\subset G_1,F_2\subset G_2,G_1\cap G_2=\varnothing$$

证明 (1) 设 F_1 有界，于是由定理 4.7.2(1) 可知 $\rho(F_1,F_2)=r>0$。令

$$G_1=\{x\mid\rho(x,F_1)<\frac{r}{2}\},G_2=\{x\mid\rho(x,F_2)<\frac{r}{2}\}$$

则由引理 4.7.1 和 4.7.2 知，G_1,G_2 都是开集，且 $F_1\subset G_1,F_2\subset G_2,G_1\cap G_2=\varnothing$。因此定理在这种情况下成立。

(2) 设

$$E_1=F_1\cap B_1,E_2=F_1\cap B_2,\cdots,E_n=F_1\cap B_n,\cdots$$

其中 $B_n=\{x\mid\rho(0,x)\leqslant n\}$，那么显然 B_n 都是有界闭集，因而 E_n 也都是有界闭集。而且

$$F_1=E_1\cup E_2\cup\cdots\cup E_n\cup\cdots$$

$$E_n\cap F_2=\varnothing,n=1,2,\cdots$$

于是由(1)中已证的结论可知

存在开集 G_{11}, G_{21},使得 $E_1 \subset G_{11}, F_2 \subset G_{21}, G_{11} \cap G_{21} = \varnothing$;

存在开集 G_{12}, G_{22},使得 $E_2 \subset G_{12}, F_2 \subset G_{22}, G_{12} \cap G_{22} = \varnothing$;

…

存在开集 G_{1n}, G_{2n},使得 $E_n \subset G_{1n}, F_2 \subset G_{2n}, G_{1n} \cap G_{2n} = \varnothing$;

…

根据引理4.7.2中开集的构造方法知道,我们可设

$$G_{11} \subset G_{12} \subset \cdots \subset G_{1n} \subset \cdots$$

$$G_{21} \subset G_{22} \subset \cdots \subset G_{2n} \subset \cdots$$

因而对任意 i,j 都有 $G_{1i} \cap G_{2j} = \varnothing$。

设 $G_1 = \bigcup_{n=1}^{\infty} G_{1n}, G_2 = \bigcup_{n=1}^{\infty} G_{2n}$,则显然 $F_1 = \bigcup_{n=1}^{\infty} E_n \subset \bigcup_{n=1}^{\infty} G_{1n} = G_1, F_2 \subset \bigcup_{n=1}^{\infty} G_{2n} = G_2$,并且 $G_1 \cap G_2 = \varnothing$,由定理4.6.1知 G_1, G_2 都是开集,这就在一般情况下(也即 F_1, F_2 不一定至少有一个是有界的情况下)证明了定理。

上面分别得到了开集和闭集的一些性质,然而并未说明二者之间有何关系。利用余集的概念可以得出它们之间的关系。

定理 4.7.4

(1) 开集的余集是闭集;

(2) 闭集的余集是开集。

证明 (1) 设 G 是开集,x_0 是 CG 的极限点,则 C 中包含一个序列 $\{x_n\}$ ($x_n \neq x_0$,当 $n \neq m$ 时,$x_n \neq x_m$),使得 $\lim\limits_{n \to \infty} x_n = x_0$。如果 $x_0 \notin CG$,那么 $x_0 \in G$,因而在 G 中存在一个包含 x_0 的开区间 K,$x_0 \subset K \subset G$。开区间 K 中显然不含有 CG 中的任何一点,因此 x_0 不可能是 CG 的极限点,这与我们的假设矛盾。所得的矛盾说明必有 $x_0 \in CG$,这就证明了 CG 是闭集。

(2) 设 F 是闭集,x_0 是 CF 中任意一点。则因为 F 的极限点都属于 F,故 x_0 不是 F 的极限点。这就是说,必存在一个包含 x_0 的开区间 K,而 K 不包含 F 中的任何点,由于 x_0 本身也不是 F 的点,因此开区间 K 整个都不属于 F,因而属于 CF,这就是说对任意 $x_0 \in CF$,CF 中都存在一个包含 x_0 的开区间 K,故 CF 是开集。

利用开集和闭集的上述关系以及集合之间的距离概念就得到:

定理 4.7.5 $\mathbf{R}$ 中的既开又闭的集合只有 $\varnothing$ 和 $\mathbf{R}$ 本身。

证明 设 A 是一个既开又闭的集合,如果 $A \neq \varnothing, A \neq \mathbf{R}$,那么 $B = CA$ 也是既开又闭的,且也有 $CA \neq \varnothing, CA \neq \mathbf{R}$。设 D 是一个线段,其一个端点 x 属于 A,而另一个端点 y 属于 B。设 $\rho(x,y) = d$,设 z 是 x,y 的中点,即设 $z = \frac{x+y}{2}$,则 $z \in D$。

关系式 $z \in A \cap D$ 或 $z \in B \cap D$ 必有一个成立，假设 $z \in A \cap D$，则

$$d = \rho(x,y) \leqslant \rho(z,y) \leqslant \frac{d}{2}$$

这显然是一个矛盾。所得的矛盾就说明不可能存在不是空集又不是 $\mathbb{R}$ 的既开又闭的集合。

为得出闭集的以下性质，我们先给出所谓“凝点”的概念。

定义 4.7.4 设 E 是一个点集，x_0 是任意一个点。如果每个包含 x_0 的开区间 (a,b) 中都含有 E 中不可数多个点，则称 x_0 为 E 的凝点。

林得勒夫(Lindelöf, Ernst Leonhard, 1870—1946)，瑞典－芬兰数学家. 生于赫尔辛基(当时为瑞典赫尔辛福斯)，卒于同地.

定理 4.7.6(林得勒夫) 如果 E 的点都不是 E 的凝点，则 E 是至多可数的。

证明 假设开区间 (a,b) 的两个端点都是有理数，而且 (a,b) 中至多含有 E 中可数多个点，则称 (a,b) 是一个正规区间。由于集合 $\{(a,b) \mid a, b$ 都是有理数$\}$ 是至多可数的(例 2.3.4(1))，因此全体正规区间是至多可数的。

任取 $x \in E$(如果 E 是空集，那么定理已经成立)，由于 x 不是 E 的凝点，因此必有开区间 (a,b) 包含 x 而 (a,b) 中至多含有 E 中可数多个点。由有理数的稠密性可知，必存在有理数 r 和 R 使得 $a < r < x < R < b$。于是按照正规区间的定义，(r,R) 就是一个正规区间，这就是说，E 中每一点都可被一个正规区间所覆盖。上面已证全体正规区间是至多可数的，因此可设全体正规区间为 $\delta_1, \delta_2, \cdots, \delta_n, \cdots E \subset \bigcup_{n=1}^{\infty} \delta_n$，而因此

$$E = \bigcup_{n=1}^{\infty} (E \cap \delta_n)$$

由于上式中并号之后的每一个集合都是至多可数的，所以就得出 E 是至多可数的。

由此定理得出

定理 4.7.7

(1) 如果 E 是不可数集合，则 E 中至少包含一个凝点。

(2) 设 E 是一个点集，P 是 E 的全体凝点组成的集合，则 $E \setminus P$ 是至多可数的。

(3) 设 E 是不可数的集合，P 是 E 的全体凝点组成的集合，那么 $E \cap P$ 是不可数的。

证明 (1)，(2) 显然，只证(3)。由于 $E \cap P = E - (E - P)$，因此由(2)已证的结论和引理 2.3.8 即得出 $E \cap P$ 是不可数的。

定理 4.7.8 设 E 是不可数的集合，则 E 的全体凝点组成的集合 P 是一个完备集。

证明 先证 P 是闭集。

设 x_0 是 P 的任一极限点，则由极限点的性质知任取包含 x_0 的开区间 (a,b)，则 (a,b) 中至少含有一个 P 的点 z。按照 P 的定义可知 z 是一个 E 的凝点，所以 (a,b) 中包含 E 的不可数多的点，这就说明 x_0 自己也是一个凝点，因而 $x_0 \in P$，所以 P 是闭集。

其次证明 P 没有孤立点，也就是要证明 P 中的每个点都是极限点。任取 $x_0 \in P$，设 (a,b) 是包含 x_0 的开区间。按照 P 的定义可知 x_0 是 E 的凝点，所以 (a,b) 中包含 E 的不可数多的点，即 $Q = E \cap (a,b)$ 是不可数集。设 R 是 Q 的全体凝点组成的集合，那么由定理4.7.7(3) 可知 $Q \cap R$ 是不可数的。因此 $Q \cap R$ 中含有不可数个 R 中的点，也就是说 $Q \cap R$ 中含有不可数个 Q 的凝点，但因为 $Q \cap R \subset Q$，所以 Q 中含有不可数个 Q 的凝点。但是 $Q \subset E$，所以 Q 的凝点就是 E 的凝点，因此 Q 中或 (a,b) 中都含有不可数个 E 的凝点，即不可数个 P 中的点，这就说明 x_0 是 P 的极限点。从 x_0 的任意性就得出 $P \subset P' \subset P$（由于已证 P 是闭的），故 $P = P'$。这就证明了 P 是完备的。

由此定理即得出

定理 4.7.9（康托尔－本迪克逊） 设 F 是不可数的闭集，则 $F = P \cup D$，其中 P 是完备集，D 是至多可数集。

本迪克逊（Bendixson, Ivor Otto, 1861—1935），挪威数学家，生于瑞典斯德哥尔摩.

证明 设 P 是 F 的所有凝点的集合，则 $P \subset F$，而 $D = F \setminus P$ 是至多可数的（定理 4.7.7(2)）。

下面我们来定义稠密性的概念。

在 4.5 中我们已了解了有理数具有稠密的特性，表现在任何两个有理数之间必存在一个有理数以及任何实数的附近都存在有理数。或者说任何一个实数都可以用有理数去逼近。这是有理数的稠密性，一般地，我们有

定义 4.7.5 设 A，B 是直线上的两个点集，如果 B 的每个点的任意邻域（即任意包含这个点的开区间）中都有 A 的点则称 A 在 B 中稠密。当 B 是全体实数 $\mathbf{R}$ 时，即 A 在全体实数中稠密时，称 A 是稠密集。

例如，$[0,1]$ 中的全体有理数在 $[0,1]$ 中稠密，而全体有理数的集合是稠密集。

和稠密性相对的概念就是不稠密，在一个局部不稠密是很容易的，这只要在一个开区间中完全不含 A 中的点，因此我们感兴趣的是哪都不稠密的概念。

定义 4.7.6 设 S 是直线上的点集，如果 S 在每个非空开集中都不稠密，则称 S 是无处稠密集。

定理 4.7.10 S 是无处稠密集的充分必要条件是对任何开区间 (a,b)，必存在一个开区间 $(a',b') \subset (a,b)$，而 (a',b') 不包含任何 S 中的点。

证明 设对任何开区间 (a,b)，必存在一个开区间 $(a',b') \subset (a,b)$，而 (a',b') 不包含任何 S 中的点。那么任取一个非空开集 G，由于 G 非空，因此 G

中必至少含有一个点 x_0，由于 G 是开集，故存在开区间 (a,b) 使得 $x_0 \in (a,b) \subset G$。根据假设，对于开区间 (a,b)，存在开区间 $(a',b') \subset (a,b)$，而 (a',b') 不包含任何 S 中的点。这就说明 S 在 G 中的点 x_0 的邻域中不稠密，故 S 在 G 中不稠密。由 G 的任意性就得出 S 是无处稠密的。

反过来，设 S 是无处稠密的，那么 S 在开集 (a,b) 中是无处稠密的。因而对于 (a,b) 中的点 x_0，必存在一个邻域 (a',b')，使得 $(a',b') \subset (a,b)$，而 (a',b') 不包含任何 S 中的点（如果不存在这样的邻域，那么 S 在点 x_0 的邻域中就是稠密的了）。这就证明了必要性。

稠密集和无处稠密集之间的关系颇像开集和闭集的关系，这就是

定理 4.7.11 无处稠密集的余集一定是稠密的。

证明 设 S 是无处稠密集，(a,b) 是任意开区间，那么根据定理 4.7.10 必存在开区间 $(a',b') \subset (a,b)$，而 (a',b') 不包含任何 S 中的点，那也就是说 (a',b') 中的点全都是 S 的余集 CS 中的点。这说明任意开区间中都含有 CS 中的点，因此 CS 是稠密的。

我们说稠密集和无处稠密集之间的关系颇像开集和闭集的关系，但只是像而不完全一样。比如说上面这个定理的逆命题就不成立。例如，设 $\mathbf{Q}$ 表示全体有理数，那么 $\mathbf{Q}$ 是稠密集，但是 $\mathbf{Q}$ 的余集是全体无理数，也是稠密的。

定理 4.7.12 如果 A 是不包含任何开区间的闭集，那么 A 一定是无处稠密集。

证明 设 (a,b) 是任意开区间，由于 A 不包含开区间，因此 (a,b) 中必含有一个点不属于 A，即 A 中必含有一个 A 的余集 CA 中的点 x_0，但是 CA 是开集，因此必存在一个存在开区间 (a',b') 使得 $x_0 \in (a',b') \subset CA$，缩小这个区间并使它始终包含 x_0，可使 $x_0 \in (a',b') \subset (a,b)$。这就是说，对于开区间 (a,b)，我们找到了一个开区间 $x_0 \in (a',b') \subset (a,b)$，而 (a',b') 中不包含任何 A 中的点，由定理 4.7.10 这就证明了 A 是无处稠密的。

我们现在再来看看完备集的一个特性。这个特性就是要不然它里面什么都没有，要不然它就一定包含很多东西。因为按照完备集的定义，空集也是完备的，这个时候它里面当然什么也没有，但是这实在是一种很特殊又很没意思的情形。如果完备集是非空的，那么它首先就包含了它的所有极限点，而每个极限点的邻域中就有无限多个这个集中的点，因此这种集合中的点肯定不会太少，更确切地说，我们有下面的定理：

定理 4.7.13 直线上任意非空完备集 A 的势是 c。

证明 由于直线上所有点的势是 c，所以只须证明 A 有一个子集的势是 c 即可。

首先，将 $(0,1]$ 中的实数表示成为无限的二进小数。

因为 A 不是空集，而且其中每个点都是自己的极限点，因此 A 中至少包含两个点，而且这两个点的距离不超过 1。把这两个点记为 x_0 和 $x_{0.1}$，并将 x_0 和 0 对应，将 $x_{0.1}$ 和 0.1 对应。再分别作 x_0 和 $x_{0.1}$ 的不相交的而且没有共同端点的邻域 U_0, U_1 并使这两个邻域的长度都不超过$\frac{1}{2}$。由于 A 是完备的，因此 A 中没有孤立点(见定理 4.7.8 的证明)，因而在 $U_0 \cap A$ 中除了 x_0 之外至少还有一点 $x_{0.01}$，而在 $U_1 \cap A$ 中除了之 $x_{0.1}$ 外至少还有一点 $x_{0.11}$。

按照邻域 U_0, U_1 的做法可知 $|x_0 - x_{0.01}| < \frac{1}{2}$，$|x_{0.1} - x_{0.11}| < \frac{1}{2}$。令 $x_{0.01}$ 对应于 0.01，$x_{0.11}$ 对应于 0.11。

同理再分别作 x_0 和 $x_{0.01}$ 的不相交的而且没有共同端点的邻域 U_{00}, U_{01}，并使这两个邻域的长度都不超过$\frac{1}{4}$，作 $x_{0.1}$ 和 $x_{0.11}$ 的不相交的而且没有共同端点的邻域 U_{10}, U_{11} 并使这两个邻域的长度都不超过$\frac{1}{4}$。于是在 $U_{00} \cap A$，$U_{01} \cap A$，$U_{10} \cap A$，$U_{11} \cap A$ 中又至少各有一个不同于此邻域中原有的点的新点 $x_{0.001}$，$x_{0.011}$，$x_{0.101}$，$x_{0.111}$，且

$$|x_0 - x_{0.001}| < \frac{1}{4}, \; |x_{0.01} - x_{0.011}| < \frac{1}{4}$$

$$|x_{0.1} - x_{0.101}| < \frac{1}{4}, \; |x_{0.11} - x_{0.111}| < \frac{1}{4}$$

如此继续下去，我们就得到点 $x_{0.i_1 i_2 \cdots i_n}(i_k = 0,1; k = 1,2,\cdots,n)$ 和邻域 $U_{i_1 i_2 \cdots i_n}(i_k = 0,1; k = 1,2,\cdots,n)$ 使得

(1) $x_{0.i_1 i_2 \cdots i_n} \in U_{i_1 i_2 \cdots i_{n-1}}$；

(2) $U_{i_1 i_2 \cdots i_{n-1} i_n} \in U_{i_1 i_2 \cdots i_{n-1}}$；

(3) $\overline{U}_{i_1, i_2, \cdots, i_n} \cap \overline{U}_{i'_1 i'_2 \cdots i'_n} = \varnothing$，$((i_1 i_2 \cdots i_n) \neq (i'_1 i'_2 \cdots i'_n))$；

(4) $U_{i_1 i_2 \cdots i_n}(i_k = 0,1; k = 1,2,\cdots,n)$ 的长度不超过$\frac{1}{2^n}$。

现在设 $a = 0.a_1 a_2 \cdots a_n \cdots$，那么从 a 可以得到一系列邻域 $U_{a_1 a_2 \cdots a_n}$。

由于 $U_{a_1 a_2 \cdots a_n}$ 的长度不超过$\frac{1}{2^n}$，而且当 $m \geqslant n$ 时，$x_{0.a_1 a_2 \cdots a_m} \in U_{a_1 a_2 \cdots a_n}$，所以当 $m, m' \geqslant n$ 时 $|x_{0.a_1 a_2 \cdots a_m} - x_{0.a_1 a_2 \cdots a_{m'}}| < \frac{1}{2^n}$，因此叙列 $x_{0.a_1}, x_{0.a_1 a_2}, \cdots, x_{0.a_1 a_2 \cdots a_m}, \cdots$ 收敛，设此叙列的极限是 y_a。但是由于 A 是完备的，因而是闭的，故必有 $y_a \in A$。

现在作全体二进无限小数到 A 上的映射 $\varphi: a \mapsto y_a$。我们证 φ 一定是单射(见第二章定义2.2.3之前的说明)。实际上如果 $a \neq b$，$b = 0.b_1 b_2 \cdots b_n \cdots$，那么

必存在一个自然数 n 使得 $a_1 = b_1, a_2 = b_2, \cdots, a_{n-1} = b_{n-1}$，但是 $a_n \neq b_n$。当 $m \geqslant n$ 时

$$x_{0.a_1a_2\cdots a_m} \in U_{a_1a_2\cdots a_{n-1}a_n}, x_{0.b_1b_2\cdots b_m} \in U_{a_1a_2\cdots a_{n-1}b_n}$$

令 $m \to \infty$，那么根据上述点和邻域的构造过程可知 y_a 总是位于 $U_{a_1a_2\cdots a_{n-1}a_n}$ 内或其端点上，y_b 总是位于 $U_{a_1a_2\cdots a_{n-1}b_n}$ 内或其端点上，而 $U_{a_1a_2\cdots a_{n-1}a_n}$ 和 $U_{a_1a_2\cdots a_{n-1}b_n}$ 不相交也没有公共端点，因此 $y_a \neq y_b$，这就证明了 φ 是单射。

设 $S = \{0.i_1i_2\cdots i_n\cdots\}$，那么由定理4.1.4可知 S 的势是 c，由于 φ 是单射，故 A 有一个子集 $\varphi((0,1]) \subset A$ 的势是 c，这就证明了 A 的势是 c。

由此定理和康托尔－本迪克逊定理(定理4.7.9)立即得到

定理 4.7.14 不可数的闭集的势一定是 c。

习题 4.7

1. 如果叙列 x_n 中有某一项 x_k 具有性质：对一切 $n \geqslant k$ 成立 $x_k \geqslant x_n$，则称 x_k 是一个山顶。利用这一概念证明，在任意叙列 $\{x_n\}$ 中必可抽出一个单调的子序列，从而证明(波查诺－维尔斯特拉斯)定理：任一有界序列 $x_1, x_2, \cdots, x_n, \cdots$ 中必存在收敛的子序列。

2. 设 (a,b) 是一个开区间。$m(a,b) = \inf\limits_{x\in(a,b)}\{f(x)\}$，$M(a,b) = \sup\limits_{x\in(a,b)}\{f(x)\}$，则称 $\omega(a,b) = M(a,b) - m(a,b)$ 是函数 $f(x)$ 在开区间 (a,b) 上的振幅。

(1) 求函数 $f(x) = x^2$ 在开区间(1,3)，(1.9,2.1)，(1.99,2.01) 以及在开区间(1.999,2.001) 上的振幅；

(2) 求函数 $f(x) = \arctan\dfrac{1}{x}$ 在开区间(1,1)，(0.1,0.1)，(0.01,0.01) 和开区间(0.001,0.001) 上的振幅。

3. 设 $\omega(h, x_0)(h > 0)$ 表函数 $f(x)$ 在开区间 $(x_0 - h, x_0 + h)$ 上的振幅。

(1) 证明：极限 $\lim\limits_{h\to0}\omega(h,x_0)$ 存在，并称 $\omega(x_0) = \lim\limits_{h\to0}\omega(h,x_0)$ 为函数 $f(x)$ 在点 x_0 的振幅；

(2) 证明：$f(x)$ 在点 x_0 为连续的充分必要条件是 $\omega(x_0) = 0$；

(3) 证明：$E = \{x \mid \omega(x) \geqslant \epsilon\}(\epsilon > 0)$ 是闭集。

4. 类似于 1. 中叙列的山顶的概念，可以定义函数 $f(x)$ 在一个开区间 (a,b) 上的山顶的概念。设 $f(x)$ 在闭区间 $[a,b]$ 上连续，令 $G = \{x \mid$ 存在 y 使 $f(y) > f(x)\}$。证明：如果 $(c,d) \subset G$，，但是 $c, d \notin G$，那么 $f(c) = f(d)$。

5. 证明：[0,1] 中所有十进小数中不含 7 的数字组成的集合是一个完备集。

6. 证明：单调函数的间断点至多有可数个。

7. 证明：任意函数的间断点所组成的集合是可数个闭集的并。

8. 设 $F_n(n=1,2,3,\cdots)$ 都是非空的有界闭集，且 $F_1\supset F_2\supset\cdots\supset F_n\supset\cdots$ 则 $\bigcap\limits_{n=1}^{\infty}F_n$ 不空。

9. 证明：任何一个闭区间 $[a,b]$ 不可能表示成可数个无处稠密集的并。

10. 黎曼函数的定义为：如果 $x=\dfrac{p}{q}$，其中 p,q 是互素的整数，$q\neq 0$，那么 $f(x)=\dfrac{1}{q}$，如果 x 是无理数，那么 $f(x)=0$。证明：黎曼函数在有理点间断，在无理点连续。

11. 证明：在 $[0,1]$ 上不可能定义一个在有理点连续，在无理点间断的函数。

12. 至少要用多少长度为 ε 的开区间才能覆盖闭区间 $[0,1]$？

13. 设 $\{I_n\}$ 是开区间的叙列，$\{I_n\}$ 覆盖了闭区间 $[0,1]$，证明：$\sum\limits_{n=1}^{\infty}|I_n|>1$。

14. 构造一个 $(0,1)$ 和 $[0,1]$ 之间的 1—1 对应。

15. 设 $A=B\cup C$，$\overline{\overline{A}}=c$，则 B 和 C 中，至少有一个集合的势是 c。

16. 设 $f(x)$ 具有性质：对每一个 x_0 都存在一个正数 $\delta>0$，使当 $|x-x_0|<\delta$ 时就有 $f(x)\geqslant f(x_0)$，那么 $f(x)$ 的函数值至多是可数集。

17. 设 $f(x)$ 是闭区间 $[a,b]$ 上的单调递增函数，$f(a)\geqslant a$，$f(b)\leqslant b$，则必存在 $\xi\in[a,b]$ 使得 $f(\xi)=\xi$。

无理数

第五章

5.1 无理数引起的震动和挑战

到现在为止，我们已经从集合论、数的小数表示和有理系数多项式的根这三个方面的证据知道了无理数的存在性。因此我们对有无理数存在这件事是丝毫不会感到有什么不自然之处，也不会因为得知这件事而感到不可思议和震惊。

但是在历史上可不是这样。

在古希腊(约公元前600年到公元600年)，文明曾一度高度发达，奴隶的劳动积累了足够的产品和财富因而使得生产、贸易、制造各业欣欣向荣，社会有条件让被称为贵族的阶层过着奢侈的生活，以及让所谓的哲人能够脱离体力劳动而专门从事思考和研究各类问题。这时人们的思想非常活跃，大到思考宇宙的本质是什么，小到研制一些具体的机械都有人去做。

古希腊在关于存在于我们之外的物质和世界究竟是什么样子的问题上也形成了两大学派，一派认为物质是无限可分的，另一派则认为物质总是由非常微小的粒子(当时称为原子，这个原子的概念和现代的以物理实验发现为基础的原子概念不是一回事，它表示这是组成物质的最终的不可再分的基础)。

虽然这两派学说都没有实际的证据而只是哲人的设想，但是用这两派学说都可以去解释一部分的现实现象，所以都各有人拥护。

按照原子论，直线是由点组成的，既然点是不可再分的，你就必然要得出这样的结论：每条直线上的点是一个整数，因而任何两条线段的比都是两个整数的比。

事实上，对应于原子论，古希腊的数学界也被一个称为毕达哥拉斯的学派所控制。毕达哥拉斯学派认为数最崇高，最神秘，他们所讲的数是指整数。"数即万物"，也就是说宇宙间各种关系都可以用整数或整数之比来表达。据说这个学派有两条最能概括他们思想特色的格言："什么最智慧？只有数目。""什么最美好？只有和谐。"毕达哥拉斯学派在数学上的一项重大贡献是证明了勾股定理。据说毕达哥拉斯在完成这一定理的证明后欣喜若狂，而杀牛百只以示庆贺。因此这一定理还又获得了一个带神秘色彩的称号："百牛定理"。

毕达哥拉斯（Pythagoras，约公元前560—480），希腊哲学家、数学家、天文学家、音乐理论家，生于萨摩斯岛，卒于梅塔蓬图姆（今意大利半岛南部塔兰托附近）。

在他们看来，这个世界是如此和谐，其表现就在于宇宙间各种关系都可以用整数或整数之比来表达。这种看法已经形成了一种不可违反的教条，不容思考和怀疑。任何敢于设想还有不能这样表示的量的企图和苗头都会被认为是异端和妖魔的想法而要受到惩罚。

但是历史的发展是不依人的意志为转移的，世界的本来面目如果不是这样，那么不管哲人们的设想是如何美妙，也早晚是要被打破和抛弃的。

历史就是这么具有喜剧性，你本来想走进这间房间，却发现现实之路把你带到了另一个房间。毕达哥拉斯所建立的毕达哥拉斯定理就是这样。就是这个使毕达哥拉斯学派的权威达到了空前地步的定理却成了毕达哥拉斯学派数学信仰的"掘墓人"。

毕达哥拉斯定理提出后，其学派中的一个成员毕达哥拉斯的学生希帕索斯考虑了一个问题：边长为 1 的正方形其对角线长度是多少呢？他发现这一长度既不能用整数，也不能用分数表示，而只能用一个新数来表示。希帕索斯的发现导致了数学史上第一个无理数$\sqrt{2}$ 的诞生。

小小$\sqrt{2}$ 的出现，却在当时的数学界掀起了一场巨大风暴。它直接动摇了毕达哥拉斯学派的数学信仰，使毕达哥拉斯学派为之大为恐慌。实际上，这一伟大发现不但是对毕达哥拉斯学派的致命打击。对于当时所有古希腊人的观念这都是一个极大的冲击。这一结论的悖论性表现在它与常识的冲突上：任何量，在任何精确度的范围内都可以表示成有理数。这不但在希腊当时是人们普遍接受的信仰，就是在今天，测量技术已经高度发展时，这个断言也毫无例外是正确的！可是为我们的经验所确信的，完全符合常识的论断居然被小小的$\sqrt{2}$ 的存在而推翻了！这应该是多么违反常识，多么荒谬的事！它简直把以前所知道的事情根本推翻了。更糟糕的是，面对这一荒谬人们竟然毫无办法。

由于触犯了这个学派的信条，毕达哥拉斯在学派内部规定了一条纪律：谁都不准泄露$\sqrt{2}$(即无理数) 存在的秘密。天真的希帕索斯有一次在海滩上无意中向别人谈到了他的发现，正好毕达哥拉斯学派的人也在海滩上并听到了他与朋友的谈话。他们发现希帕索斯泄密，违反了学派的纪律。结果把希帕索斯扔到大海里淹死。这说明这一发现对当时的权威的振动有多大，已达到了不惜杀人灭口的程度。

但$\sqrt{2}$ 很快就引起了数学思想的大革命。希帕索斯为$\sqrt{2}$ 殉难留下的教训是：科学是没有止境的，谁为科学划定禁区，谁就变成科学的敌人，最终被科学所埋葬。这就在当时直接导致了人们认识上的危机，从而导致了西方数学史上一场大的风波，史称"第一次数学危机"。

这场"危机" 表明，直觉和经验不一定靠得住，推理证明才是可靠的。从此以后，希腊人开始由重视计算转向重视推理，由重视算术转向重视几何学，并由此建立了几何公理体系。其实，这是数学思想上的一次巨大革命！

毕达哥拉斯学派的观念牵涉公度的概念：

定义 5.1.1 两个量 a 和 b 称为是可公度的，如果存在着第三个量 c，使得 a 和 b 都可以表示为 c 的整数倍数，即存在整数 m 和 n 使得 $a = mc, b = nc$。

由前面所讲过的内容容易得出

定理 5.1.1 两个量 a 和 b 是可公度的充分必要条件是

(1) $\frac{a}{b}, b \neq 0$ 是有理数；或

(2) 设 $b > 0$，对 a 和 b 实行的辗转相除法可在有限步内结束。

实际上希帕索斯最初的发现表达的形式就是正方形的边长和对角线是不可公度的，而无理数的发现表明现实世界中存在着不可公度的量。无理数这个词的本义就是不可表示，这个词的本来含义恰反映了当初人们发现无理数存在时的无奈和不知所措。

但是与西方形成鲜明对照的是当时中国的思想界，在西方的数学界为以往的错误观念遇到了障碍而出现了多次危机时(这种危机不止一次地出现过，仅数学界就出现过 3 次，如果再算上思想界、宗教界和文学界中出现的冲突就更多了)，在中国却从未由于数学概念或宗教见解的不同而闹到要杀人的地步。这主要是中国的科学太注重实用而缺乏理性的思维。从实用的角度看，有理数和无理数没有本质的区别，都是需要不断精确化的数量，所以我们的祖冲之的重要成就也就是用一个很好的分数$\frac{355}{113}$ 去逼近无理数 π。当西方为了宗教信仰而发生所谓胡格诺战争 —— 圣巴托罗缪之夜大屠杀，胡斯战争，十字军东征等为了信仰的战争时，中国内部发生的却是为了实际利益而争夺不断的宗族械斗，为了抢夺政权而战的农民战争，对外发生的是不断地抗击侵略的战争，直到近

代才有为了主义的不同而发生的内战。

这也应该是一个教训，即科学研究不能是专门为了实用才进行，这样会阻碍科学的发展。科学也需要解决它内部自身提出的问题才能得到正常的发展。的确，当人们思考是否存在不可公度的量时，还根本不知道这一思考会有什么用，但是历史表明，对这一问题的深入思考促进了数学的发展，也最终为数学的应用打下了很好的基础。这样的例子还有很多，例如概率论发展的初期完全看不到有什么实用意义，它一开始研究的问题是赌博问题，但是后来却得到了广泛的应用。要求科学研究的成果立刻获得实际应用是一种短视的观点。

5.2 一些初等函数值的无理性

所谓初等函数，就是由幂函数、指数函数、对数函数、三角函数这些最基本的函数经过加减乘除、迭代这些运算所得的函数。

我们所关注的问题是，如果 x 是有理数，那么在什么情况下 $f(x)$ 仍是有理数。

首先考虑幂函数和指数函数，如果 x 是有理数，m 是整数，那么显然 x^m 仍是有理数。所以我们进一步考虑 m 是有理数的情况，在这种情况下，通过一系列化简，我们最终会得到一个形如 $r\sqrt[n]{m}$ 的式子，其中 r 是一个有理数，m 是整数。于是问题化为研究在什么情况下$\sqrt[n]{m}$ 是有理数的问题。

定理 5.2.1 整系数多项式 $f(x)=x^n+a_1x^{n-1}+\cdots+a_n$ 的有理根必是一个整数，且此整数必是 a_n 的因子。

证明 设 $f(x)$ 存在有理根 $r=\dfrac{p}{q}$，其中 p,q 是互素的整数，$q\neq 0$。则由定理 4.4.1 可知必有 $p\mid a_n$，$q\mid 1$。由此可知 $r=p$ 是整数，且此整数必是 a_n 的因子。

由此立得：

定理 5.2.2 如果 m 不是一个整数的 n 次方，则$\sqrt[n]{m}$ 必是一个无理数。

证明 $\sqrt[n]{m}$ 是整系数多项式 $f(x)=x^n-m$ 的根，此多项式当且仅当 m 是一个整数的 n 次方时才有整数根。因而由定理 5.2.1 就证明了当 m 不是一个整数的 n 次方时，$\sqrt[n]{m}$ 必是一个无理数。

用反证法易证下面的

定理 5.2.3 设 α 是无理数，r 是有理数，则 $\alpha+r,\alpha-r,r\alpha,\dfrac{\alpha}{r}(r\neq 0)$ 都是无理数，也就是说无理数和有理数通过四则运算（除数不等于零）所得的结果是无理数。

两个无理数通过四则运算(除数不等于零)所得的结果一般不能保证仍是一个无理数。例如$\sqrt{2}+(-\sqrt{2})=0$。$\sqrt{2}-\sqrt{2}=0$,$\sqrt{2}\cdot\sqrt{2}=2$,$\frac{\sqrt{2}}{\sqrt{2}}=1$都不是无理数。但是我们在许多特殊的情况下,可以证明如此运算所得的结果仍是无理数。

例 5.2.1 证明:$\sqrt{2}+\sqrt{3}$是无理数。

证明 设$x=\sqrt{2}+\sqrt{3}$,则$x-\sqrt{2}=\sqrt{3}$,因此

$$x^2-2\sqrt{2}x+2=3,x^2-1=2\sqrt{2}x$$

把此式两边再平方一次并合并同类项即可知x是多项式

$$x^4-10x^2+1$$

的根。由定理4.4.1知其整数根只可能是1或-1,极易通过验算得知它们均不是上述多项式的根,因此多项式x^4-10x^2+1没有整数根,因而由定理5.2.1即得$x=\sqrt{2}+\sqrt{3}$必是无理数。

例 5.2.2 证明:$\sqrt[3]{2}-\sqrt{3}$是无理数。

证明 设$x=\sqrt[3]{2}-\sqrt{3}$,则$x+\sqrt{3}=\sqrt[3]{2}$,将此式两边3次方,并将有理项和无理项分离可得

$$x^3+9x-2=-\sqrt{3}(x^2+1)$$

再将此式两边平方并合并同类项即可知x是多项式

$$x^6-9x^4-4x^3+27x^2-36x-23$$

的根。此多项式的整数根只可能是± 1和± 23。仍然通过直接验算可知它们都不是上述多项式的根,因此多项式$x^6-9x^4-4x^3+27x^2-36x-23$不存在整数根。故由定理5.2.1即得$x=\sqrt[3]{2}-\sqrt{3}$是无理数。

现在来考虑对数函数,我们有:

定理5.2.4 设$p>0,q>0,(p,q)=1$,则当且仅当$\frac{p}{q}=10^n,n=0,\pm 1,\pm 2,\cdots$时,$\log\frac{p}{q}$是一个有理数。

证明 设$\log\frac{p}{q}=\frac{a}{b},b>0$是一个有理数。于是由对数的意义即得$10^{\frac{a}{b}}=\frac{p}{q}$,因而$q\cdot 10^{\frac{a}{b}}=p,q^b10^a=p^b$。

以下分两种情况进行讨论。

(1) $a\geqslant 0$。这时如果$q\neq 1$,则由上式可得$(p^b,q^b)>1$,但是由$(p,q)=1$又得出$(p^b,q^b)=1$。这一矛盾说明必须$q=1$,因此$p^b=10^a$。设$p=10^np',n\geqslant 0$,其中p'中不含有因子10,那么$10^{nb}(p')^b=10^a$,由此式得出必须$p'=1,a=nb,p=10^n$。

(2) $a<0$。这时由$q^b10^a=p^b$得出$q^b=p^b10^{-a},-a>0$。于是和(1)中同

理可证 $p = 1, q = 10^n, n > 0$。

综合(1),(2) 的论证就得出 $\frac{p}{q} = 10^n, n = 0, \pm 1, \pm 2, \cdots$

当 $\frac{p}{q} = 10^n, n = 0, \pm 1, \pm 2, \cdots$ 时,显然 $\log \frac{p}{q}$ 是一个有理数,这就完全证明了定理。

由此定理可知 $\log \frac{3}{2}$, $\log 15$ 以及 $\log 3 + \log 5$ 都是无理数。

还有一种对数函数 $\ln x$ 称为自然对数,这种对数的底通常用 e 来标记。其中

$$e = \lim_{n \to \infty}\left(1 + \frac{1}{n}\right)^n = 1 + 1 + \frac{1}{2!} + \frac{1}{3!} + \cdots$$

由于 e 本身的性质就比较复杂,我们就不在此讨论 $\ln x$ 的无理性了,以后可以证明 e 本身就是一个无理数,$\ln 2$ 也是一个无理数。

现在来讨论三角函数的无理性,首先证明两个引理。

引理 5.2.1 $2\cos(n+1)\theta = 4\cos n\theta\cos\theta - 2\cos(n-1)\theta$。

证明 由三角公式中的两角和公式得出

$$\begin{aligned}&2\cos(n+1)\theta + 2\cos(n-1)\theta = \\&2(\cos n\theta\cos\theta - \sin n\theta\sin\theta + \cos n\theta\cos\theta + \sin n\theta\sin\theta) = \\&4\cos n\theta\cos\theta\end{aligned}$$

再把 $2\cos(n-1)\theta$ 移到等式右边就得到这个引理。

引理 5.2.2 设 $x = 2\cos\theta$, n 是一个自然数,则

$$2\cos n\theta = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$$

其中,$a_1, a_2, \cdots, a_n$ 都是整数。

证明 当 $n = 1$ 时,根据我们的假设就有 $2\cos\theta = x$,命题成立;当 $n = 2$ 时

$$2\cos 2\theta = 2(2\cos^2\theta - 1) = 4\cos^2\theta - 2 = (2\cos\theta)^2 - 2 = x^2 - 2$$

命题也成立,因此引理中的命题对于自然数 $n = 1, 2$ 都成立。

现在假设命题对一切小于或等于 n 的自然数都成立,于是可设

$$2\cos(n-1)\theta = x^n + b_1x^{n-1} + \cdots + b_{n-2}x + b_{n-1}$$

$$2\cos n\theta = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$$

其中 $b_1, b_2, \cdots, b_{n-1}, a_1, a_2, \cdots, a_n$ 都是整数。于是根据引理 5.2.1 和归纳法假设就得到

$$\begin{aligned}2\cos(n+1)\theta &= 4\cos n\theta\cos\theta - 2\cos(n-1)\theta = \\&2\cos\theta(2\cos n\theta) - 2\cos(n-1)\theta = \\&x(x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n) -\end{aligned}$$

$$(x^n + b_1x^{n-1} + \cdots + b_{n-2}x + b_{n-1}) =$$
$$x^{n+1} + c_1x^n + c_2x^{n-1} + \cdots + c_nx + c_{n+1}$$

其中 $c_1 = a_1, c_2 = a_2 - 1, c_3 = a_3 - b_1, \cdots, c_n = a_n - b_{n-2}, c_{n+1} = -b_{n-1}$ 都是整数，这就说明在归纳法假设成立的条件下，命题对自然数 $n+1$ 仍然成立。因此由数学归纳法就证明了对一切自然数命题成立，这就证明了引理。

定理 5.2.5 设 $\theta = \frac{p}{q}, q > 0$ 是一个有理数（单位是度），$0° \leqslant \theta \leqslant 90°$，则

(1) 当且仅当 $\theta = 0°, 60°, 90°$ 时，$\cos\theta$ 是有理数；

(2) 当且仅当 $\theta = 0°, 30°, 90°$ 时，$\sin\theta$ 是有理数；

(3) 当且仅当 $\theta = 0°, 45°$ 时，$\tan\theta$ 是有理数。

证明 (1) 假设 $\cos\theta$ 是有理数，则显然 $2\cos\theta$ 也是有理数。

设 $n = 360°q$，则 $n\theta = 360°p$ 是 $360°$ 的倍数，因此 $\cos n\theta = 1$，将 $\cos n\theta = 1$ 代入

$$2\cos n\theta = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$$

并移项可知 $2\cos\theta$ 是多项式

$$x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n - 2$$

的有理根，因此根据定理 5.2.1 可知 $2\cos\theta$ 必是上面的多项式的整数根。由于 $0° \leqslant \theta \leqslant 90°$，故 $0 \leqslant 2\cos\theta \leqslant 2$，因而 $2\cos\theta$ 只能等于 0,1,2，这就得出 $\theta = 0°, 60°, 90°$。反过来显然 $\cos 0° = 1, \cos 60° = \frac{1}{2}, \cos 90° = 0$ 都是有理数，这就证明了(1)。

(2) 由 $\sin\theta = \cos(90° - \theta)$ 和(1)已证的结论即可得出(2)。

(3) 利用 $\cos\theta = -\cos(180° - \theta)$ 和(1)已证明的结论，可知如果 $0° \leqslant \theta \leqslant 180°$，则当且仅当 $\theta = 0°, 60°, 90°, 120°, 180°$ 时，$\cos\theta$ 是有理数。

现在设 $0° \leqslant \theta \leqslant 90°$，则 $0° \leqslant 2\theta \leqslant 180°$。

如果 $\tan\theta$ 是有理数，那么 $\tan^2\theta$ 也是有理数，因此 $\frac{1-\tan^2\theta}{1+\tan^2\theta} = \cos 2\theta$ 也是有理数，因此根据上面的讨论 $\frac{1-\tan^2\theta}{1+\tan^2\theta}$ 只可能取 $\cos 0° = 1, \cos 60° = \frac{1}{2}, \cos 90° = 0, \cos 120° = -\frac{1}{2}$ 和 $\cos 180° = -1$ 这 5 个值。

依次让 $\frac{1-\tan^2\theta}{1+\tan^2\theta}$ 等于 $1, \frac{1}{2}, 0, -\frac{1}{2}$ 和 -1，并解相应的方程再结合 $0° \leqslant \theta \leqslant 90°$ 的条件（因此 $\tan\theta \geqslant 0$），我们得到 $\theta = 0°, 30°, 45°, 60°$ 这 4 个解，但是反过来只有 $\tan 0°$ 和 $\tan 45°$ 是有理数，所以满足 θ 和 $\tan\theta$ 都是有理数的解就只有 $\theta = 0°$ 和 $\theta = 45°$ 这两个，这就证明了定理。

最后我们可以提出，如果 α 有理数，β 是无理数，那么 α^β 是什么数？如果 α

和β都是无理数，α^β是否一定是无理数？更一般地，可以问如果α是代数数，$\alpha\neq 0,1$，β是一个无理的代数数，α^β是否一定是一个代数数，这就是1900年，著名数学家大卫·希尔伯特在第二届国际数学家大会上提出的著名的23个数学问题中的第7个问题。这一问题首先在1929年被苏联著名数学家A·O·盖里冯德所突破，他证明了如果α是代数数，$\alpha\neq 0,1$，β是虚二次无理数，那么α^β一定是一个超越数（因此当然是一个无理数）。1930年，苏联数学家R·O·库兹明又将A·O·盖里冯德的结果推广到β是实二次无理数的情况。到1934年A·O·盖里冯德和Th.施奈德各自独立地完全解决了希尔伯特第七问题。

根据他们的结果，我们就可以断定$e^\pi=(-1)^{-i}, 2^{\sqrt{2}}, \sqrt{2}^{\sqrt{2}}$等数都是超越数，因而都是无理数。但是以上结果的证明实在是太高深，太难了，因此我们只能在本书中提一下最后的结果而无法介绍这些结果的证明，有兴趣的读者可以参看朱尧辰，徐广善所著的《超越数引论》一书。

由上面的说明可以知道，判断形如α^β的数是有理数还是无理数一般是非常复杂的，因此下面的例子就尤其值得注意。

例 5.2.3 存在无理数α,β而使得α^β是有理数。

证明 分以下两种情况进行讨论。

(1) $\sqrt{2}^{\sqrt{2}}$是有理数，这时只要取$\alpha=\beta=\sqrt{2}$即可；

(2) $\sqrt{2}^{\sqrt{2}}$是无理数，这时只要取$\alpha=\sqrt{2}^{\sqrt{2}}$，$\beta=\sqrt{2}$，那么

$$\alpha^\beta=(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}}=(\sqrt{2})^{\sqrt{2}\cdot\sqrt{2}}=(\sqrt{2})^2=2$$

故这时$\alpha=\sqrt{2}^{\sqrt{2}}$，$\beta=\sqrt{2}$就符合要求。

因此，无论发生那种情况，所说的无理数都是存在的。

当然，这两种情况是不可能同时发生的，根据以上所说的盖里冯德定理可知实际发生的是第二种情况。但是以上证明的妙处就在于它不需要引用像盖里冯德定理这样很高深的结果。

5.3 对称多项式

韦 达（Vieta, Francois, 1540—1603），法国数学家．生于法国东部地区的普瓦图，卒于巴黎．

假设$x_1,x_2,\cdots,x_n$是多项式$f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n$的所有根，那么根据代数基本定理，$f(x)$就可以分解成为一次因式的乘积如下

$$f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n=a_0(x-x_1)(x-x_2)\cdots(x-x_n)$$

把上面的等式的右边展开并比较等式两边同类项的系数就可得出以下定理：

定理 5.3.1（韦达） 根与系数的关系。

设 $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$，它的所有的根是 $x_1, x_2, \cdots, x_n$，那么

$$x_1 + x_2 + \cdots + x_n = -\frac{a_1}{a_0}$$

$$x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n = \frac{a_2}{a_0}$$

$$\vdots$$

$$x_1x_2\cdots x_n = (-1)^n\frac{a_n}{a_0}$$

在根与系数的关系定理中出现的 n 个关于 $x_1, x_2, \cdots, x_n$ 的多项式具有这样的特点，即无论怎样调换这些多项式中变元的相互位置，这些多项式都不变，像这样的多项式就称为对称多项式。下面我们给出它的严格定义：

定义 5.3.1 集合 $\{1, 2, \cdots, n\}$ 到自身的一个 1—1 的变换称为一个 n 元置换。

例如，$\tau(1) = 2, \tau(2) = 4, \tau(3) = 1, \tau(4) = 3$ 就是一个 4 元置换。

一个 n 元置换 τ 可以用表

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \tau(1) & \tau(2) & \cdots & \tau(n) \end{pmatrix}$$

来表示。例如，上面的 4 元置换就可表示为

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 2 \end{pmatrix}$$

既然置换是 1—1 的变换，所以 $\tau(1), \tau(2), \cdots, \tau(n)$ 就是 $1, 2, \cdots, n$ 的一个排列，由此可知所有 n 元置换的个数就等于 n 元排列的个数，也就是 $n!$.

定义 5.3.2 如果对任意一个 n 元置换都有

$$f(x_1, x_2, \cdots, x_n) = f(x_{\tau(1)}, x_{\tau(2)}, \cdots, x_{\tau(n)})$$

则称 $f(x_1, x_2, \cdots, x_n)$ 是 $x_1, x_2, \cdots, x_n$ 的对称函数，当 $f(x_1, x_2, \cdots, x_n)$ 是 $x_1, x_2, \cdots, x_n$ 的多项式时，就称 $f(x_1, x_2, \cdots, x_n)$ 是 $x_1, x_2, \cdots, x_n$ 的对称多项式。

定义 5.3.3 以下 n 个对称多项式称为初等对称多项式

$$\sigma_1 = x_1 + x_2 + \cdots + x_n$$

$$\sigma_2 = x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n$$

$$\vdots$$

$$\sigma_n = x_1x_2\cdots x_n$$

由对称多项式的定义可知成立下面的

引理 5.3.1 对称多项式的多项式还是对称多项式，即如果 $f_1, f_2, \cdots, f_n$ 都是 $x_1, x_2, \cdots, x_n$ 的对称多项式，而 $g(y_1, y_2, \cdots, y_n)$ 是任一 n 元多项式，那么 $g(f_1, f_2, \cdots, f_n)$ 就也是 $x_1, x_2, \cdots, x_n$ 的对称多项式。

特别地，初等对称多项式的多项式还是对称多项式。

为了证明关于对称多项式的基本结果，下面我们首先给出多元的单项式之间的一种顺序，由于这种排序方法类似于字典的排列原则，因而称为字典排列法。

定义 5.3.4 如果以下 n 个数

$$k_1 - l_1, k_2 - l_2, \cdots, k_n - l_n$$

中第一个不为 0 的数是正的，也就是说，存在 $i \leqslant n$，使得

$$k_1 - l_1 = 0, \cdots, k_{i-1} - l_{i-1} = 0, k_i - l_i > 0$$

则称 n 元数组 $(k_1, k_2, \cdots, k_n)$ 先于 n 元数组 $(l_1, l_2, \cdots, l_n)$，并记为

$$(k_1, k_2, \cdots, k_n) > (l_1, l_2, \cdots, l_n)$$

例如，$(1,3,2) > (1,2,4)$。

从上面这个定义容易看出有

引理 5.3.2 定义 5.3.4 中所给出的关系“>”是 n 元数组之间的一个次序，即若 α, β 设是任意两个 n 元数组，则“>”关系具有以下性质：

(1) 在三种关系 $\alpha > \beta, \alpha = \beta, \alpha < \beta$ 之中必有一种关系成立，且仅有一种关系成立；

(2) 若 $\alpha > \beta, \beta > \gamma$，则 $\alpha > \gamma$（传递性）。

定义 5.3.5 如果 $(k_1, k_2, \cdots, k_n) > (l_1, l_2, \cdots, l_n)$，则称按字典排列法，单项式 $x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}$ 在单项式 $x_1^{l_1} x_2^{l_2} \cdots x_n^{l_n}$ 之前。

例如，多项式 $2x_1x_2^2x_3^2 + x_1^2x_2 + x_1^3$ 按字典排列法写出来就是 $x_1^3 + x_1^2x_2 + 2x_1x_2^2x_3^2$。

定义 5.3.6 一个多项式按照字典排列法写出来后第一个系数不为 0 的项称为此多项式的首项。

由上面的例子可以看出，首项的次数不一定是最大的。首项有下面的性质：

引理 5.3.3 设 f, g 都是关于 $x_1, x_2, \cdots, x_n$ 的多项式，且 $f \neq 0, g \neq 0$，那么 fg 的首项就等于 f 的首项和 g 的首项的乘积。

证明 设 f 中任意单项式的形式为 $x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}$，首项为 $ax_1^{p_1} x_2^{p_2} \cdots x_n^{p_n}, a \neq 0$，$g$ 中任意单项式的形式为 $x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}$，首项为 $bx_1^{q_1} x_2^{q_2} \cdots x_n^{q_n}, b \neq 0$，那么乘积 fg 中的任意单项式的方幂共可能对应于以下三种类型的 n 元数组

$$\text{Ⅰ}: (p_1 + k_1, p_2 + k_2, \cdots, p_n + k_n)$$

$$\text{Ⅱ}: (l_1 + k_1, l_2 + k_2, \cdots, l_n + k_n)$$

$$\text{Ⅲ}: (l_1 + q_1, l_2 + q_2, \cdots, l_n + q_n)$$

由于 $ax_1^{p_1} x_2^{p_2} \cdots x_n^{p_n}, a \neq 0$ 和 $bx_1^{q_1} x_2^{q_2} \cdots x_n^{q_n}, b \neq 0$ 分别是 f, g 的首项，因此

$$(p_1, p_2, \cdots, p_n) > (l_1, l_2, \cdots, l_n)$$

$$(q_1,q_2,\cdots,q_n) > (k_1,k_2,\cdots,k_n)$$

显然

$$(p_1+q_1,p_2+q_2,\cdots,p_n+q_n) > (p_1+k_1,p_2+k_2,\cdots,p_n+k_n)$$
$$(p_1+q_1,p_2+q_2,\cdots,p_n+q_n) > (l_1+q_1,l_2+q_2,\cdots,l_n+q_n)$$

由传递性又有

$$(p_1+q_1,p_2+q_2,\cdots,p_n+q_n) > (l_1+q_1,l_2+q_2,\cdots,l_n+q_n) > (l_1+k_1,l_2+k_2,\cdots,l_n+k_n)$$

因此,根据字典排列法的规则,乘积 fg 的首项就应该对应于数组$(p_1+q_1,p_2+q_2,\cdots,p_n+q_n)$,也即乘积 fg 的首项为 $abx_1^{p_1+q_1}x_2^{p_2+q_2}\cdots x_n^{p_n+q_n}$,而这一项就是 f 的首项和 g 的首项的乘积,这就证明了引理。

由此引理立即得出

定理 5.3.2

(1) 设 $f_i, i=1,2,\cdots,m$ 都是关于 $x_1,x_2,\cdots,x_n$ 的多项式,$f_i\neq 0$,那么 $f_1f_2\cdots f_m$ 的首项就等于每个 f_i 的首项的乘积;

(2) 设 f,g 都是关于 $x_1,x_2,\cdots,x_n$ 的多项式,且 $f\neq 0, g\neq 0$,那么 $fg\neq 0$。

定义 5.3.7 设 f 是关于 $x_1,x_2,\cdots,x_n$ 的多项式,如果组成 f 的每个单项式都是 m 次的,就称 f 是 $x_1,x_2,\cdots,x_n$ 的 m 次齐次多项式。

容易验证,齐次多项式具有如下性质:

引理 5.3.4 设 f 是关于 $x_1,x_2,\cdots,x_n$ 的多项式,那么 f 是 $x_1,x_2,\cdots,x_n$ 的 m 次齐次多项式的充分必要条件是

$$f(tx_1,tx_2,\cdots,tx_n) = t^m f(x_1,x_2,\cdots,x_n)$$

显然,任何一个 $x_1,x_2,\cdots,x_n$ 的 m 次多项式 f 都可以唯一地表示成

$$f(x_1,x_2,\cdots,x_n) = \sum_{i=0}^{m} f_i(x_1,x_2,\cdots,x_n)$$

的形式,其中 $f_i(x_1,x_2,\cdots,x_n)$ 是 i 次的齐次多项式,也就是说任何一个 m 次多项式 f 都可以分解为齐次多项式之和。

下面我们给出对称多项式的重要性质。

引理 5.3.5 设 f 是关于 $x_1,x_2,\cdots,x_n$ 的对称多项式,f 的按字典排列法规则订出的首项是 $ax_1^{l_1}x_2^{l_2}\cdots x_n^{l_n}, a\neq 0$,那么必有 $l_1\geqslant l_2\geqslant\cdots\geqslant l_n\geqslant 0$。

证明 用反证法,假设引理的结论不成立,那么必有使得上式不成立的脚标存在,令 i 是使得 $l_i<l_{i+1}$ 成立的最小脚标。那么由于 f 含有 $ax_1^{l_1}x_2^{l_2}\cdots x_i^{l_i}x_{i+1}^{l_{i+1}}\cdots x_n^{l_n}, a\neq 0$ 项,故由 f 的对称性,f 必也含有 $ax_1^{l_1}x_2^{l_2}\cdots x_i^{l_{i+1}}x_{i+1}^{l_i}\cdots x_n^{l_n}, a\neq 0$ 项(后者可以由前者通过交换 x_i 和 x_{i+1} 的位置而得到,而根据对称多项式的定义可知,任意交换位置数的位置所有的多项式不变,

因此 f 必含有这一项，否则 f 不可能不变），而根据字典排列法，如此一来 $ax_1^{l_1}x_2^{l_2}\cdots x_i^{l_{i+1}}x_{i+1}^{l_i}\cdots x_n^{l_n}$ 就应该位于 $ax_1^{l_1}x_2^{l_2}\cdots x_i^{l_i}x_{i+1}^{l_{i+1}}\cdots x_n^{l_n}$ 之前，这与 $ax_1^{l_1}x_2^{l_2}\cdots x_i^{l_i}x_{i+1}^{l_{i+1}}\cdots x_n^{l_n}$ 是 f 的首项矛盾，所得的矛盾就证明了引理的结论。

定理5.3.3(对称多项式基本定理)　任意 n 元对称多项式 $f(x_1,x_2,\cdots,x_n)$ 都可用 $x_1,x_2,\cdots,x_n$ 的 n 个初等对称多项式 $\sigma_1,\sigma_2,\cdots,\sigma_n$ 唯一地表出。

证明　设对称多项式 $f(x_1,x_2,\cdots,x_n)$ 按字典排列法得出的首项为 $ax_1^{l_1}x_2^{l_2}\cdots x_n^{l_n}$，$a\neq 0$。我们作一个多项式 $g_1=a\sigma_1^{l_1-l_2}\sigma_2^{l_2-l_3}\cdots\sigma_n^{l_n}$，由于 $\sigma_1,\sigma_2,\cdots,\sigma_n$ 的首项分别为 $x_1,x_1x_2,\cdots,x_1x_2\cdots x_n$，所以根据定理5.3.2可知我们上面所作的多项式的首项就是

$$ax_1^{l_1-l_2}(x_1x_2)^{l_2-l_3}\cdots(x_1x_2\cdots x_n)^{l_n}=ax_1^{l_1}x_2^{l_2}\cdots x_n^{l_n}$$

这就是说 $f(x_1,x_2,\cdots,x_n)$ 和我们所作的多项式的首项是相同的。因而对称多项式

$$f_1(x_1,x_2,\cdots,x_n)=f(x_1,x_2,\cdots,x_n)-a\sigma_1^{l_1-l_2}\sigma_2^{l_2-l_3}\cdots\sigma_n^{l_n}=f-g_1$$

的首项按字典排列法应位于 $a\sigma_1^{l_1-l_2}\sigma_2^{l_2-l_3}\cdots\sigma_n^{l_n}$ 之后。而 g_1 可由初等对称多项式表出。

对 $f_1(x_1,x_2,\cdots,x_n)$ 又可重复上面的作法，又可得到一个对称多项式 $f_2=f_1-g_2$，其首项按字典排列法位于 f_1 的首项之后，而 g_2 可由初等对称多项式表出。

这种手续可以继续进行下去，可以得到一系列的对称多项式

$$f_1=f-g_1$$
$$f_2=f_1-g_2$$
$$\vdots$$

按照我们的做法可知，它们的首项的位置按字典排列法一个比一个靠后，而 g_i 可由初等对称多项式表出。

由首项的定义和定理5.3.3得出这一系列多项式的首项中每个字母的指数都不会超过 l_1，因此所有这种首项的个数是有限的，因而我们所得出的一系列对称多项式 $f,f_1,f_2,\cdots$ 之中也只能有有限个对称多项式不为零，这也就是说，必存在一个自然数 h 使得 $f_h=0$。因而就有

$$\begin{aligned}f=f_1+g_1&=g_1+g_2+f_2=\cdots=\\&g_1+g_2+\cdots+g_h+f_h=\\&g_1+g_2+\cdots+g_n\end{aligned}$$

由于 $g_1,g_2,g_3,\cdots$ 都可用初等对称多项式表出，这就证明了 f 也可用初等对称多项式表出。

下面证明上面已证的表示方法是唯一的。

所谓唯一性是指由 $f(x_1,x_2,\cdots,x_n)\neq g(x_1,x_2,\cdots,x_n)$ 可以得出 $f(\sigma_1,\sigma_2,\cdots,\sigma_n)\neq g(\sigma_1,\sigma_2,\cdots,\sigma_n)$。由于$f(x_1,x_2,\cdots,x_n)\neq g(x_1,x_2,\cdots,x_n)$等价于 $f(x_1,x_2,\cdots,x_n)-g(x_1,x_2,\cdots,x_n)\neq 0$。因此只须证明由 $f(x_1,x_2,\cdots,x_n)\neq 0$ 可以得出 $f(\sigma_1,\sigma_2,\cdots,\sigma_n)\neq 0$ 即可。

用反证法。设 $f(\sigma_1,\sigma_2,\cdots,\sigma_n)=0$,且至少 $f(\sigma_1,\sigma_2,\cdots,\sigma_n)$ 中有一个单项式的系数不为零(这就是说 $f(\sigma_1,\sigma_2,\cdots,\sigma_n)=0$ 不是 $0=0$,或者说 $\sigma_1,\sigma_2,\cdots,\sigma_n$ 之间有一个多项式形式的隐含关系式)。设这一项是 $a\sigma_1^{k_1}\sigma_2^{k_2}\cdots\sigma_n^{k_n}$,$a\neq 0$。把这一项中所有的 σ_i 换成$x_1,x_2,\cdots,x_n$ 的表达式就得到一个 $x_1,x_2,\cdots,x_n$ 的多项式。由定理 5.3.2 可知这一多项式的首项是

$$ax_1^{k_1}(x_1x_2)^{k_2}\cdots(x_1x_2\cdots x_n)^{k_n}=ax_1^{k_1+k_2+\cdots+k_n}x_2^{k_2+k_3+\cdots+k_n}\cdots x_n^{k_n}$$

如果 $ax_1^{k_1+k_2+\cdots+k_n}x_2^{k_2+k_3+\cdots+k_n}\cdots x_n^{k_n}$ 和 $bx_1^{l_1+l_2+\cdots+l_n}x_2^{l_2+l_3+\cdots+l_n}\cdots x_n^{l_n}$ 是同类项,那么显然就有

$$\begin{aligned}k_1+k_2+\cdots+k_n&=l_1+l_2+\cdots+l_n\\k_2+\cdots+k_n&=l_2+\cdots+l_n\\&\vdots\\k_n&=l_n\end{aligned}$$

因而由解方程组就可得出必有$(k_1,k_2,\cdots,k_n)=(l_1,l_2,\cdots,l_n)$,故 $a\sigma_1^{k_1}\sigma_2^{k_2}\cdots\sigma_n^{k_n}$ 与 $b\sigma_1^{l_1}\sigma_2^{l_2}\cdots\sigma_n^{l_n}$ 是同类项。这就是说 $f(\sigma_1,\sigma_2,\cdots,\sigma_n)$ 中两个不同的项化成的 $x_1,x_2,\cdots,x_n$ 的多项式的首项不会是同类项。

于是把多项式 $f(\sigma_1,\sigma_2,\cdots,\sigma_n)$ 的每一项写成 $x_1,x_2,\cdots,x_n$ 的多项式后,这些多项式的首项不可能互相抵消,因此在这些首项中按字典排列法有一个位于最前面的项,这一项显然也在所化成的 $x_1,x_2,\cdots,x_n$ 的多项式中的任意项之前。

这样我们从 $\sigma_1,\sigma_2,\cdots,\sigma_n$ 之间有一个多项式形式的隐含关系式 $f(\sigma_1,\sigma_2,\cdots,\sigma_n)=0$就得出 $x_1,x_2,\cdots,x_n$之间的一个多项式形式的隐含关系式$f(x_1,x_2,\cdots,x_n)=0$,而且由于其首项不为零,因此 $f(x_1,x_2,\cdots,x_n)=0$ 不是 $0=0$。这就是说,变量 $x_1,x_2,\cdots,x_n$ 不是互相独立的。而这与我们的基本假设矛盾。这就证明了唯一性。

例 5.3.1 把 $x_1^3+x_2^3+x_3^3$ 表成 $\sigma_1,\sigma_2,\sigma_3$ 的多项式。

解 按照定理5.3.3的证明方法,我们肯定可以把 $x_1^3+x_2^3+x_3^3$表成 $\sigma_1,\sigma_2,\sigma_3$ 的多项式。然而具体去确定这一表示式时,由于已经知道这种表示方法存在,我们可以采用其他方法,例如待定系数法。

由于 $x_1^3+x_2^3+x_3^3$ 是3次齐次对称多项式,而由 $\sigma_1,\sigma_2,\sigma_3$ 共可做成3个3次齐次多项式 $\sigma_1^3,\sigma_1\sigma_2,\sigma_3$,因此可设

$$x_1^3+x_2^3+x_3^3=a\sigma_1^3+b\sigma_1\sigma_2+c\sigma_3$$

在上式中令 $x_1=1,x_2=x_3=0$ 即得 $x_1^3=ax_1^3$,因此 $a=1$。

把 $a=1$ 代入上式,并再令 $x_1=1,x_2=1,x_3=0$ 即得 $2=8+2b$,因此 $b=3$。

把 $a=1,b=3$ 代入上式,并再令 $x_1=1,x_2=1,x_3=1$ 即得 $3=27-27+c$,因此 $c=3$,故

$$x_1^3+x_2^3+x_3^3=\sigma_1^3-3\sigma_1\sigma_2+3\sigma_3$$

现考虑一元多项式 $f(x)=a_0x^m+a_1x^{m-1}+\cdots+a_m$。

定义 5.3.8 设 $f(x)=a_0x^m+a_1x^{m-1}+\cdots+a_m$ 的所有根是 $\alpha_1,\alpha_2,\cdots,\alpha_m$,则称

$$D(f)=a_0^{2(m-1)}\prod_{i<j}(\alpha_i-\alpha_j)^2$$

为 $f(x)=a_0x^m+a_1x^{m-1}+\cdots+a_m$ 的判别式。

定理 5.3.4 $f(x)$ 有重根的充分必要条件是 $D=0$。

证明 根据 D 的定义即可知 $f(x)$ 有重根的充分必要条件是 $D=0$。

例 5.5.2 当 $n=2$ 时,$f(x)=a_0x^2+a_1x+a_2$。

$$D=a_0^2(\alpha_2-\alpha_1)^2=a_0^2((\alpha_2+\alpha_1)^2-4\alpha_1\alpha_2)=$$
$$a_0^2\left(\left(-\frac{a_1}{a_0}\right)^2-4\left(\frac{a_2}{a_0}\right)\right)=a_1^2-4a_0a_2$$

例 5.3.3 当 $n=3$ 时,$f(x)=a_0x^3+a_1x^2+a_2x+a_3$。

解 这时用对称函数基本定理的证明方法可以求出

$$D=a_0^4(\sigma_1^2\sigma_2^2-4\sigma_1^3\sigma_3-4\sigma_2^3+18\sigma_1\sigma_2\sigma_3-27\sigma_3^2)=$$
$$a_0^4\left(\left(-\frac{a_1}{a_0}\right)^2\left(\frac{a_2}{a_0}\right)^2-4\left(-\frac{a_1}{a_0}\right)^3\left(-\frac{a_3}{a_0}\right)-4\left(\frac{a_2}{a_0}\right)^3+\right.$$
$$\left.18\left(-\frac{a_1}{a_0}\right)\left(\frac{a_2}{a_0}\right)\left(-\frac{a_3}{a_0}\right)-27\left(-\frac{a_3}{a_0}\right)^2\right)=$$
$$a_1^2a_2^2-4a_1^3a_3-4a_0a_2^3+18a_0a_1a_2a_3-27a_0^2a_3^2$$

现在考虑两个多项式

$$f(x)=a_0x^m+a_1x^{m-1}+\cdots+a_m$$
$$g(x)=b_0x^n+b_1x^{n-1}+\cdots+b_m$$

定义 5.3.9 设 $a_0\neq0,f(x)=a_0x^m+a_1x^{m-1}+\cdots+a_m$ 的所有根是 $\alpha_1,\alpha_2,\cdots,\alpha_m,b_0\neq0,g(x)=b_0x^n+b_1x^{n-1}+\cdots+b_n$ 的所有根是 $\beta_1,\beta_2,\cdots,\beta_n$,则称

$$R(f,g)=a_0^nb_0^m\prod_{i=1}^m\prod_{j=1}^n(\alpha_i-\beta_j)$$

为多项式 $f(x)$ 和 $g(x)$ 的结式。

定理 5.3.5

(1) $R(f,g)=a_0^n g(\alpha_1)g(\alpha_2)\cdots g(\alpha_m)=b_0^m f(\beta_1)f(\beta_2)\cdots f(\beta_n)$；

(2) $R(f,g)$ 可由 $f(x)$ 和 $g(x)$ 的系数表出；

(3) 多项式 $f(x)$ 和 $g(x)$ 有公共根的充分必要条件是 $R(f,g)=0$。

证明 (1)

$$f(x)=a_0(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_m)$$
$$g(x)=b_0(x-\beta_1)(x-\beta_2)\cdots(x-\beta_n)$$

于是

$$f(\beta_j)=a_0(\beta_j-\alpha_1)(\beta_j-\alpha_2)\cdots(\beta_j-\alpha_m)=(-1)^n(\alpha_1-\beta_j)(\alpha_2-\beta_j)\cdots(\alpha_m-\beta_j)$$
$$g(\alpha_i)=b_0(\alpha_i-\beta_1)(\alpha_i-\beta_2)\cdots(\alpha_i-\beta_n)$$

因而

$$R(f,g)=a_0^n b_0^m\prod_{i=1}^{m}\prod_{j=1}^{n}(\alpha_i-\beta_j)=a_0^n g(\alpha_1)g(\alpha_2)\cdots g(\alpha_m)=(-1)^{mn}b_0^m f(\beta_1)f(\beta_2)\cdots f(\beta_n)$$

(2) 由(1)可见 $R(f,g)$ 既是 $\alpha_1,\alpha_2,\cdots,\alpha_m$ 的对称多项式又是 $\beta_1,\beta_2,\cdots,\beta_n$ 的对称多项式，因此既可由 $\alpha_1,\alpha_2,\cdots,\alpha_m$ 的初等对称多项式和 $g(x)$ 的系数表出又可由 $\beta_1,\beta_2,\cdots,\beta_n$ 的初等对称多项式和 $f(x)$ 的系数表出，因而再由根与系数的关系，$R(f,g)$ 可由 $f(x)$ 的系数和 $g(x)$ 的系数表出。

(3) 由 $R(f,g)$ 的定义即可得出。

习题 5.3

1. 用初等对称多项式表出下列对称多项式

(1) $x_1^2x_2+x_1x_2^2+x_1^2x_3+x_1x_3^2+x_2^2x_3+x_2x_3^2$

(2) $(x_1+x_2)(x_2+x_3)(x_1+x_3)$

(3) $(x_1-x_2)^2(x_2-x_3)^2(x_3-x_1)^2$

(4) $x_1^2x_2^2+x_1^2x_3^2+x_1^2x_4^2+x_2^2x_3^2+x_2^2x_4^2+x_3^2x_4^2$

(5) $(x_1x_2+x_3)(x_2x_3+x_1)(x_1x_3+x_2)$

(6) $(x_1+x_2+x_1x_2)(x_2+x_3+x_2x_3)(x_1+x_3+x_1x_3)$

2. 用初等对称多项式表出下列 n 元对称多项式

(1) $\sum x_1^4$

(2) $\sum x_1^2x_2x_3$

(3) $\sum x_1^2x_2^2$

(4) $\sum x_1^2x_2^2x_3x_4$

($\sum ax_1^{l_1}x_2^{l_2}\cdots x_k^{l_k}$ 表示所有由 $ax_1^{l_1}x_2^{l_2}\cdots x_k^{l_k}$ 经过置换得到的项的和)

3. 用初等对称多项式表出下列对称函数

(1) $\sum_{i=1}^{n}\frac{1}{x_i^2}$　　(2) $\sum_{i,j=1}^{n}\frac{x_j}{x_i}$

4. 计算下列各组多项式的结式

(1) $\begin{cases}x^3-3x^2+2x+1\\2x^2-x-1\end{cases}$　　(2) $\begin{cases}2x^3-3x^2-x+2\\x^4-2x^2-3x=4\end{cases}$

(3) $\begin{cases}a_0x^n+a_1x^{n-1}+\cdots+a_n\\a_0x^{n-1}+a_1x^{n-2}+\cdots+a_{n-1}\end{cases}$

(4) $\begin{cases}x^n+1\\(x-1)^n\end{cases}$　　(5) $\begin{cases}x^n-a^n\\x^n-b^n\end{cases}$

5. 证明：$R(f,g)=(-1)^{mn}R(g,f)$。

6. 证明：$R(f,g_1g_2)=R(f,g_1)R(f,g_2)$。

7. 用数学归纳法证明

$$R(f,g)=\begin{vmatrix}a_0 & a_1 & \cdots & a_n & & & \\ & a_0 & a_1 & \cdots & a_n & & \\ & & \cdots & & & & \\ & & & a_0 & a_1 & \cdots & a_n\\ b_0 & b_1 & \cdots & b_m & & & \\ & b_0 & b_1 & \cdots & b_m & & \\ & & \cdots & & & & \\ & & & b_0 & b_1 & \cdots & b_m\end{vmatrix}$$

(上面的行列式共有 $m+n$ 行，$m+n$ 列，上面是 m 行，下面是 n 行)

5.4　代数数和超越数

前面已证$\sqrt{2}+\sqrt{3}$ 和$\sqrt[3]{2}-\sqrt{3}$ 都是无理数，然而这种无理数在全体无理数中又是具有一些独特性质，因而和一般的无理数是有所区别的。这里所谓它们是具有一些独特性质是指它们分别满足代数方程 $x^4-10x^2+1=0$ 和 $x^6-9x^4-4x^3+27x^2-36x-23=0$。像这种满足代数方程的数就称为代数数。有理数$\frac{p}{q}$，$q>0$ 显然满足代数方程 $qx-p=0$，因此所有的有理数都是代数数，因而代数数乃是有理数概念的推广。下面我们给出正式的定义。

定义 5.4.1 如果一个数 α 满足代数方程

$$a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = 0$$

其中 $a_0, a_1, \cdots, a_n$ 都是整数,则称数 α 是一个代数数。

我们还可以将整数的概念加以推广,所谓整数,当然首先是有理数,因而所有的整数都满足一个一次方程,然而整数和一般的有理数相区别的特性是整数必可满足一个最高次项的系数为 1 的整系数代数方程,把此特性推广到一般,就得到所谓代数整数的概念:

定义 5.4.2 如果一个数 α 满足一个最高次项系数为 1 的代数方程

$$x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = 0$$

其中 $a_1, \cdots, a_n$ 都是整数,则称数 α 是一个代数整数。

如果 α 是一个代数数,那么根据自然数的最小数原理,它所满足的整系数方程中必有次数最低者,因此它所满足的最低的整系数方程的次数就称为代数数 α 的次数。

定义 5.4.3 如果 α 数满足一个 n 次的代数方程

$$a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = 0$$

其中 $a_0, a_1, \cdots, a_n$ 都是整数,但是不满足任何次数低于 n 的代数方程,则称 α 是一个 n 次代数数。

定义 5.4.4 不是代数数的数称为超越数。换句话说,如果数 α 不能满足任何次数的代数方程,则称 α 是一个超越数。

显然超越数必是无理数。

为了以后证明的方便,我们首先对代数数给出一个等价的说法。

引理 5.4.1 α 是一个代数数的充分必要条件是 α 是一个首项系数为 1,其他各项系数都是有理数的代数方程的根。

证明 如果 α 是一个代数数,则根据代数数的定义,α 是一个整系数代数方程的根,用最高项的系数除以方程的各项,就得出 α 是一个首项系数为 1,其他各项系数都是有理数的代数方程的根。

反之,如果 α 是一个首项系数为 1,其他各项系数都是有理数的代数方程的根。那么在方程两边乘以各项系数的分母的最小公倍数,就得出 α 是一个整系数代数方程的根,因此 α 是一个代数数。

代数数有一些很好的性质使得我们愿意把它们从一般的无理数中区分出来单独加以研究,其中最基本的性质是所谓自封性。为说明此性质,首先证明两个引理。

引理 5.4.2 如果 α 是一个代数数,则它的相反数 $-\alpha$ 仍然是一个代数数。

证明 设 α 是一个代数数,那么 α 必满足一个整系数代数方程

$$a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = 0$$

通过直接验证可知 $-\alpha$ 满足整系数代数方程

$$a_0x^n - a_1x^{n-1} + \cdots + (-1)^{n-1}a_{n-1}x + (-1)^n a_n = 0$$

因此 $-\alpha$ 仍然是一个代数数。

引理 5.4.3 如果 $\alpha \neq 0$ 是一个代数数,则它的倒数 $\frac{1}{\alpha}$ 仍然是一个代数数。

证明 设 α 是一个代数数,并设 α 的次数为 n,那么 α 必满足一个整系数代数方程

$$a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = 0$$

由于 $\alpha \neq 0$,因此 a_n 必不能为 0,否则将有 $a_0\alpha^n + a_1\alpha^{n-1} + \cdots + a_{n-1}\alpha = 0$,由此得出 α 将满足代数方程 $a_0\alpha^{n-1} + a_1\alpha^{n-2} + \cdots + a_{n-1}x = 0$,而这与 α 的次数为 n 相矛盾。

通过直接验证可知 $\frac{1}{\alpha}$ 满足整系数代数方程

$$a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0$$

因此 $\frac{1}{\alpha}$ 仍然是一个代数数。

定理 5.4.1 两个代数数经过加、减、乘、除(除数不为 0)后仍得到代数数。

证明 设 α 和 β 都是代数数。根据引理 5.4.1 和引理 5.4.2 我们只须证明 $\alpha+\beta$ 和 $\alpha\beta(\beta \neq 0)$ 仍是代数数即可(在 $\beta = 0$ 的情况,显然 $\alpha\beta$ 仍是代数数)。又根据引理 5.4.1 我们可设 α 满足 n 次代数方程 $f(x) = 0$,β 满足 m 次代数方程 $g(x) = 0$。其中

$$f(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$$
$$g(x) = x^m + b_1x^{m-1} + \cdots + b_{m-1}x + b_m$$

这里 $a_1, a_2, \cdots, a_n$ 和 $b_1, b_2, \cdots, b_m$ 都是有理数。

根据代数基本定理,可设 $f(x) = 0$ 的所有根为 $\alpha_1, \alpha_2, \cdots, \alpha_n$,$g(x) = 0$ 的所有根为 $\beta_1, \beta_2, \cdots, \beta_m$(当然 α 和 β 也包括在 $\alpha_1, \alpha_2, \cdots, \alpha_n$ 和 $\beta_1, \beta_2, \cdots, \beta_m$ 之中),于是

$$f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$$
$$g(x) = (x-\beta_1)(x-\beta_2)\cdots(x-\beta_n)$$

我们看多项式

$$h(x) = \prod_{i=1}^{n}\prod_{j=1}^{m}(x-(\alpha_i+\beta_j)) =$$
$$\prod_{j=1}^{m}((x-\beta_j)-\alpha_1)((x-\beta_j)-\alpha_2)\cdots((x-\beta_j)-\alpha_n) =$$
$$\prod_{j=1}^{m}f(x-\beta_j)$$

显然 $\alpha+\beta$ 是 $h(x)$ 的根，并且 $h(x)$ 是 $\beta_1,\beta_2,\cdots,\beta_m$ 的有理系数对称多项式，因此根据对称多项式的基本定理，其系数都是 $\beta_1,\beta_2,\cdots,\beta_m$ 的初等对称多项式的有理系数多项式，而根据根与系数的关系可知 $\beta_1,\beta_2,\cdots,\beta_m$ 的初等对称多项式都是有理数，因而 $h(x)$ 的系数全都是有理数。根据引理 5.4.1 这就证明了 $\alpha+\beta$ 是代数数。

再看多项式

$$
\begin{aligned}
k(x) = & \prod_{i=1}^{n}\prod_{j=1}^{m}(x-\alpha_i\beta_j) = \\
& \prod_{j=1}^{m}\beta_j^n\left(\frac{x}{\beta_j}-\alpha_1\right)\left(\frac{x}{\beta_j}-\alpha_2\right)\cdots\left(\frac{x}{\beta_j}-\alpha_n\right) = \prod_{j=1}^{m}\beta_j^n f\left(\frac{x}{\beta_j}\right) = \\
& \prod_{j=1}^{m}(x^n+a_1\beta_j x^{n-1}+\cdots+a_{n-1}\beta_j^{n-1}x+a_n\beta_j^n)
\end{aligned}
$$

由此可知，$k(x)$ 也是 $\beta_1,\beta_2,\cdots,\beta_m$ 的有理系数对称多项式，因而其系数也都是有理数，并且显然 $\alpha\beta(\beta\neq 0)$ 是 $k(x)$ 的根，于是根据引理 5.4.1 就得出 $\alpha\beta(\beta\neq 0)$ 也是代数数。这就证明了定理。

最后，我们来证明代数数的封闭性。其实上面所证明的定理也是一种封闭性，不过指的是代数数对于四则运算是封闭的。现在所要证明的封闭性是指在代数数的定义中，如果把多项式的系数都换成代数数，则我们仍然得到代数数。

在数的概念每一次扩张时，我们都会遇到是否有封闭性的问题。例如，当还没有负数时，我们就无法解方程 $x+a=0, a\geqslant 0$。因此我们定义了负数，而一旦引进了负数之后，我们就要问，通过解方程 $x+a=0$，其中 a 是正数或负数或者零还会不会又出现新的数？(或者问有了负数的概念后，解方程 $x+a=0$ 还会不会有障碍？) 答案是不会。这就是一种封闭性。当还没有分数时，我们就无法解任意一个方程 $ax+b=0$，其中 a,b 都是整数。因此我们定义了分数乃至有理数，而一旦引进了有理数后，我们就要问通过解方程 $ax+b=0$，其中 a，b 都是有理数还会不会又出现新的数？答案是不会，这又是一次封闭性。当还没有实数时，我们就无法表示正方形的对角线的长度或解方程 $x^2=2$，后来我们通过有理数的极限引进了实数。而一旦引进了实数后，我们就要问对实数的序列取极限后会不会又产生新的数，答案是不会，因此实数对极限运算是封闭的。

现在我们通过解整系数代数方程引进了代数数，因此我们还要问，如果把代数方程的系数都换成代数数，又会不会产生新的数？这次的答案仍然是不会，也就是说，我们有：

定理 5.4.2 设 $f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n=0, a_0\neq 0$ 的系数都是代数数，那么 $f(x)$ 的根仍是代数数。

证明 设 α 是 $f(x)$ 的根，因而 $f(\alpha)=0$。

由于代数数的和、差、积、商（分母不为零）仍是代数数，因此我们不妨设 $a_0=1$。

根据假设和引理5.4.1我们可设 $g_i(a_i)=0$，其中 $g_i(x)$ 是首项系数为1的有理系数多项式。我们再进一步设 $g_i(x)$ 的次数为 m_i，它的所有的根是 a_i，$a_i^{(2)},\cdots,a_i^{(m_i)}$。令

$$f_0(x;a_1^{(k_1)},a_2^{(k_2)},\cdots,a_n^{(k_n)})=x^n+a_1^{(k_1)}x^{n-1}+\cdots+a_{n-1}^{(k_{n-1})}x+a_n^{(k_n)}$$

$$F(x)=\prod_{k_1=1}^{m_1}\cdots\prod_{k_n}^{m_n}f_0(x;a_1^{(k_1)},a_2^{(k_2)},\cdots,a_n^{(k_n)})$$

由对称多项式基本定理和根与系数的关系可知多项式

$$\prod_{k_1=1}^{m_1}f_0(x;a_1^{(k_1)},a_2^{(k_2)},\cdots,a_n^{(k_n)})$$

的系数是 $x,a_2^{(k_2)},\cdots,a_n^{(k_n)}$ 的有理系数多项式，所以可以记

$$\prod_{k_1=1}^{m_1}f_0(x;a_1^{(k_1)},a_2^{(k_2)},\cdots,a_n^{(k_n)})=f_1(x;a_2^{(k_2)},\cdots,a_n^{(k_n)})$$

同理以此类推可以知道多项式

$$\prod_{k_i=1}^{m_i}f_i(x;a_i^{(k_i)},a_{i+1}^{(k_{i+1})},\cdots,a_n^{(k_n)})$$

的系数是 $x,a_{i+1}^{(k_{i+1})},\cdots,a_n^{(k_n)}$ 的有理系数多项式，所以可以记

$$\prod_{k_i=1}^{m_i}f_i(x;a_i^{(k_i)},a_{i+1}^{(k_{i+1})},\cdots,a_n^{(k_n)})=f_{i+1}(x;a_{i+1}^{(k_{i+1})},\cdots,a_n^{(k_n)})$$

最后得到

$$F(x)=\prod_{k_n=1}^{m_n}f_i(x;a_n^{(k_n)})=f_n(x)$$

是有理系数多项式，由于 $f(\alpha)=0$，故由 $F(x)$ 的定义就得出 $F(\alpha)=0$。这就证明了 α 仍然是一个代数数。

习题 5.4

1. 求出 $\alpha=\sqrt{2}+\sqrt[3]{2}$ 所满足的整系数多项式方程。
2. 求出 $\alpha=\sqrt{2}+\sqrt{3}-\sqrt{6}$ 所满足的整系数多项式方程。
3. 求出 $\alpha=(1+\sqrt{3})\sqrt[3]{2}$ 所满足的整系数多项式方程。
4. 证明：$\dfrac{\sqrt{3}+\sqrt{7}}{2}$ 是代数整数。
5. 证明：两个代数整数的和、差以及积仍为一个代数整数，并举例说明商不一定是。

6. 求出方程 $x^2+\sqrt[3]{2}x+\sqrt{3}=0$ 的根 α 所满足的整系数多项式方程。

7. 设 $f(x)=x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n=0$ 的系数都是代数整数，那么 $f(x)$ 的根仍是代数整数。

8. 设 $\epsilon\neq 0$ 是一个代数整数，如果它的倒数 $\frac{1}{\epsilon}$ 也是一个代数整数，则称 ϵ 是一个单位数。证明：$3-2\sqrt{2}, 1+\sqrt[3]{2}+\sqrt[3]{2^2}, 4+3\sqrt[3]{3}+2\sqrt[3]{3^2}$ 都是单位数。

9. 证明：如果 $f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n=0, a_0\neq 0$ 的系数都是代数整数，且 a_0, a_n 都是单位数，则 $f(x)$ 的根仍是单位数。

连分数

第六章

6.1 什么是连分数

我们已知道了分数和小数，在这一章里我们要介绍一种数的新的表示方法：连分数。

定义 6.1.1 表达式

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots + \cfrac{1}{a_n}}}$$

称为 n 阶的有限连分数。其中 a_0 为任意实数，$a_1, \cdots, a_n$ 为正实数。如果 a_0 是任意整数，$a_1, \cdots, a_n$ 是正整数，则称它为 n 阶的简单连分数。

为了书写的便利和表达简单起见，一般用下面的符号来表示一个连分数，即

$$[a_0; a_1, a_2, \cdots, a_n]$$

有限连分数显然是有意义的，它的值一般是一个实数，而简单连分数的值是一个有理数。为了使上面的表达式在有无限多个元素的情况下也可以有意义，我们给出下面的定义：

定义 6.1.2 设 $a_0,a_1,\cdots,a_n,\cdots$ 是一个无穷叙列，其中 a_0 为任意实数。$a_1,\cdots,a_n,\cdots$ 为正实数。如果叙列 $a_0,[a_0;a_1],\cdots,[a_0;a_1,a_2,\cdots,a_n],\cdots$ 存在有限的极限 α，则称表达式

$$[a_1,\cdots,a_n,\cdots] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots + \cfrac{1}{a_n + \ddots}}}$$

收敛，这时，上面的表达式又称为是一个无限连分数，它的值就是 α。当 a_0 是任意整数，$a_1,\cdots,a_n,\cdots$ 是正整数时，则称它为简单无限连分数。

定义 6.1.3 $[a_0]=\dfrac{a_0}{1},[a_0;a_1]=\dfrac{p_1}{q_1},\cdots,[a_0;a_1,a_2,\cdots,a_k]=\dfrac{p_k}{q_k}$ 称为有限连分数 $[a_0;a_1,a_2,\cdots,a_n]$ 或无限连分数 $[a_0;a_1,a_2,\cdots,a_n,\cdots]$ 的第 $1,2,\cdots,k$ 阶渐近分数。

$r_k=[a_k;a_{k+1},\cdots,a_n]$ 称为是有限连分数 $[a_0;a_1,a_2,\cdots,a_n]$ 的第 k 阶余式，而 $r_k=[a_k;a_{k+1},\cdots,a_n,\cdots]$ 则称为是无限连分数 $[a_0;a_1,a_2,\cdots,a_n,\cdots]$ 的第 k 阶余式。

显然，无限的余式和无限连分数同时有意义或同时无意义。

定义任意一个符号，都首先要研究这一符号本身有些什么性质，才能开展进一步的研究，否则，我们将始终停留在把一种符号换成另一种符号去写的水平上。下面，我们就首先给出连分数符号的最基本性质。由连分数的定义通过直接验证即可知道成立下面的引理。

引理 6.1.1 设 α 表示一个有限或无限连分数，则对任意整数 $k\geqslant 1$，成立

$$\alpha = [a_0;a_1,a_2,\cdots,a_{k-1},r_k] = [a_0;a_1,a_2,\cdots,a_{k-1},a_k+\frac{1}{r_{k+1}}]$$

特别

$$[a_0;a_1,a_2,\cdots,a_n,a_{n+1}] = [a_0;a_1,a_2,\cdots,a_{n-1},a_n+\frac{1}{a_{n+1}}]$$

引理 6.1.2 设 $a_i>0,i=1,2,\cdots,n,\eta>0,\alpha_n=[a_0;a_1,a_2,\cdots,a_n]$，则

(1) 如果 n 是奇数，那么 $\alpha_n>[a_0;a_1,a_2,\cdots,a_{n-1},a_n+\eta]$；

如果 n 是偶数，那么 $\alpha_n<[a_0;a_1,a_2,\cdots,a_{n-1},a_n+\eta]$。

(2)
$$\alpha_1>\alpha_3>\cdots>\alpha_{2n-1}>\cdots$$
$$\alpha_0<\alpha_2<\cdots<\alpha_{2n}<\cdots$$

证明 (1) 当 $n=1$ 时

$$\alpha_1=[a_0;a_1]=a_0+\frac{1}{a_1}>a_0+\frac{1}{a_1+\eta}=[a_0;a_1+\eta]$$

因此这时(1) 中的第一个式子成立。假设此式对所有小于或者等于 $2n-1$ 的奇数都成立,那么

$$\alpha_{2n+1}=[a_0;a_1,\cdots,a_{2n+1}]=[a_0;a_1,[a_2;\cdots,a_{2n+1}]]$$

由于$[a_2;a_3,\cdots,a_{2n+1}]$中分号后面共有 $2n-1$ 个元素,因此由归纳法假设就有

$$\xi=[a_2;a_3,\cdots,a_{2n+1}]>[a_2;a_3,\cdots,a_{2n+1}+\eta]=\xi_n$$

故

$$\alpha_{2n+1}=[a_0;a_1,\xi]=a_0+\cfrac{1}{a_1+\cfrac{1}{\xi}}>a_0+\cfrac{1}{a_1+\cfrac{1}{\xi_n}}=$$

$$[a_0;a_1,[a_2;a_3,\cdots,a_{2n+1}+\eta]]=$$

$$[a_0;a_1,a_2,\cdots,a_{2n+1}+\eta]$$

因此由数学归纳法就证明了(1) 中的第一个式子,同理可证(1) 中的另一个式子。

(2) 由引理 6.1.1 和(1) 中已证明的式子就有

$$\alpha_1=[a_0;a_1]>[a_0;a_1+\frac{1}{[a_2;a_3]}]=[a_0;a_1,[a_2;a_3]]=$$

$$[a_0;a_1,a_2,a_3]=\alpha_3>\alpha_5>\alpha_7>\cdots$$

$$\alpha_0=[a_0]>[a_0+\frac{1}{[a_1;a_2]}]=[a_0;[a_1;a_2]]=$$

$$[a_0;a_1,a_2]=\alpha_2<\alpha_4<\alpha_6<\cdots$$

下面来考虑连分数的计算问题。

根据上面所给出的连分数的性质,对一个有限连分式,我们可以从它的最后一个元素按照连分数的定义,逐步写出一个连分数的最后表达式来。不过这样计算有一个不方便之处,就是当再添加一个元素时,一切都要从头算起,而以前所得的计算结果完全无用,另外,这样计算连分数也无法得出一个一般的明显公式。因此我们首先关注的问题是是否有一个这样的公式。

定理 6.1.1 设 $\alpha_n=\frac{p_n}{q_n}$,那么

(1) 当 $n\geqslant 2$ 时,$\begin{cases}p_n=a_np_{n-1}+p_{n-2}\\ q_n=a_nq_{n-1}+q_{n-2}\end{cases}$;

(2) $\alpha=[a_0;a_1,a_2,\cdots]=\frac{p_{k-1}r_k+p_{k-2}}{q_{k-1}r_k+q_{k-2}},k\geqslant 1$;

(3) $\frac{p_n}{p_{n-1}}=[a_n;a_{n-1},\cdots,a_0]$;

$\frac{q_n}{q_{n-1}}=[a_n;a_{n-1},\cdots,a_1]$。

证明 (1) 由直接计算可知

$$\frac{p_0}{q_0}=\frac{a_0}{1},\frac{p_1}{q_1}=\frac{a_0a_1+1}{a_1},\frac{p_2}{q_2}=\frac{a_0a_1a_2+a_2+a_0}{a_1a_2+1}$$

故
$$p_2=a_0a_1a_2+a_2+a_0=a_2(a_0a_1+1)+a_0=a_2p_1+p_0$$
$$q_2=a_1a_2+1=a_2q_1+q_0$$

因此公式对 $n=2$ 的情况成立。现在假设对一切适合 $2\leqslant k\leqslant n$ 的自然数 k 公式成立，即假设当 $n\geqslant 2$ 时

$$p_n=a_np_{n-1}+p_{n-2}$$
$$q_n=a_nq_{n-1}+q_{n-2}$$

那么 $\alpha_{n+1}=[a_0;a_1,a_2,\cdots,a_n,a_{n+1}]=[a_0;a_1,\cdots,a_{n-1},a_n+\dfrac{1}{a_{n+1}}]=\alpha'_n$

α_{n+1} 连同它本身共有 $n+2$ 个渐进分数 $\alpha_0,\alpha_1,\cdots,\alpha_{n-1},\alpha_n,\alpha_{n+1}$，而 α'_n 连同它本身共有 $n+1$ 个渐进分数 $\alpha'_0,\alpha'_1,\cdots,\alpha'_{n-1},\alpha'_n$。注意根据渐近分数的定义就可知连分数 α_{n+1} 和 α'_n 的前 $n-1$ 阶渐近分数是完全相同的，即

$$\alpha_0=\frac{p_0}{q_0}=\frac{p'_0}{q'_0}=\alpha'_0$$

$$\alpha_1=\frac{p_1}{q_1}=\frac{p'_1}{q'_1}=\alpha'_1$$

$$\vdots$$

$$\alpha_{n-1}=\frac{p_{n-1}}{q_{n-1}}=\frac{p'_{n-1}}{q'_{n-1}}=\alpha'_{n-1}$$

而由于 α'_n 已经是 n 阶连分式，故由归纳法假设就有

$$\frac{p_{n+1}}{q_{n+1}}=\alpha_{n+1}=\alpha'_n=\frac{p'_n}{q'_n}=\frac{a'_np'_{n-1}+p'_{n-2}}{a'_nq'_{n-1}+q'_{n-2}}=$$

$$\frac{\left(a_n+\dfrac{1}{a_{n+1}}\right)p_{n-1}+p_{n-2}}{\left(a_n+\dfrac{1}{a_{n+1}}\right)p_{n-1}+p_{n-2}}=\frac{a_{n+1}(a_np_{n-1}+p_{n-2})+p_{n-1}}{a_{n+1}(a_nq_{n-1}+q_{n-2})+q_{n-1}}=$$

$$\frac{a_{n+1}p_n+p_{n-1}}{a_{n+1}q_n+q_{n-1}}$$

故由数学归纳法可知，此公式对一切大于等于 2 的自然数成立。

(2) $[a_0;a_1,\cdots]=[a_0;a_1,\cdots,a_{k-1},r_k]$。因此由(1) 中已证的公式就得出(2)。

(3) 当 $n=1$ 时，$\dfrac{p_1}{p_0}=\dfrac{a_0a_1+1}{a_0}=a_1+\dfrac{1}{a_0}=[a_1;a_0]$，要证的公式成立。

假设对自然数 n 公式成立，即 $\dfrac{p_n}{p_{n-1}}=[a_n;a_{n-1},\cdots,a_0]$，那么

$$\frac{p_{n+1}}{p_n}=\frac{a_{n+1}p_n+p_{n-1}}{p_n}=a_{n+1}+\frac{1}{\frac{p_n}{p_{n-1}}}=a_{n+1}+\frac{1}{[a_n;a_{n-1},\cdots,a_0]}=$$

$$[a_{n+1};[a_n;a_{n-1},\cdots,a_0]]=[a_{n+1};a_n,a_{n-1},\cdots a_0]$$

故由数学归纳法，(3) 中的公式对一切自然数成立。同理可证(3) 中的另一个式子。

现在来看相邻的渐近分数之间有什么关系。我们有

定理 6.1.2

(1) $q_np_{n-1}-p_nq_{n-1}=(-1)^n$;

(2) $q_np_{n-2}-p_nq_{n-2}=(-1)^{n-1}a_n$。

证明

(1)
$$\begin{aligned}q_np_{n-1}-p_nq_{n-1}&=(a_nq_{n-1}+q_{n-2})p_{n-1}-(a_np_{n-1}+p_{n-2})q_{n-1}=\\&(-1)(q_{n-1}p_{n-2}-p_{n-1}q_{n-2})=\\&(-1)^2(q_{n-2}p_{n-3}-p_{n-2}q_{n-3})=\cdots=\\&(-1)^{n-1}(q_1p_0-p_1q_0)=(-1)^n\end{aligned}$$

(2)
$$\begin{aligned}q_np_{n-2}-p_nq_{n-2}&=(a_nq_{n-1}+q_{n-2})p_{n-2}-(a_np_{n-1}+p_{n-2})q_{n-2}=\\&a_n(q_{n-1}p_{n-2}-p_{n-1}q_{n-2})=\\&(-1)^{n-1}a_n\end{aligned}$$

引理 6.1.3 设$[a_0;a_1,a_2,\cdots,a_n,\cdots]$是一个任意的简单的有限或无限连分数，$\frac{p_k}{q_k}(k=0,1,\cdots)$是它的渐近分数，那么

(1) 当 $k\geqslant 2$时，$q_k\geqslant q_{k-1}+1$，因而对任意 k 有$q_k\geqslant k-1$，当 $k\to\infty$ 时，$q_k\to\infty$;

(2) $\frac{p_k}{q_k}(k=0,1,\cdots)$都是既约分数。

证明 (1) 由定理6.1.1(1)，q_k的定义和简单连分数的定义显然就有$q_k\geqslant 1$(注意这里用到了 q_k 的定义，虽然 p_k 和 q_k 的递推公式是一样的，但是由于 a_0 可以是任意整数，所以只有 q_k 才有性质q_k，而 p_k 却没有这一性质)。由于当 $k\geqslant 1$ 时，$a_k\geqslant 1$，因此当 $k\geqslant 2$ 时

$$q_k=a_kq_{k-1}+q_{k-2}\geqslant q_{k-1}+1$$

然后由 $q_0=1,q_1=a_1\geqslant 1$ 和数学归纳法即可证明(1) 的结论。

(2) 由定理 6.1.2(1)$q_np_{n-1}-p_nq_{n-1}=(-1)^n$ 即得(2)。

习题 6.1

1. 计算以下连分数的值和各阶渐近分数

(1)[1;2,3]　　(2)[0;1,2,3]　　(3)[3;2,1]

(4)[2;1,1,4,1,1]　　(5)[4;2,1,7,8]

2. 把下面的有理数表示成有限的简单连分数，并求出各阶渐近分数

(1) $\frac{121}{21}$　　(2) $-\frac{19}{29}$　　(3) $\frac{177}{292}$　　(4) $\frac{873}{4\,867}$

3. 求有限简单连分数[1;1,1,1,1,1,1,1,1,1,1]的各阶渐近分数。

4. 设 $\alpha=[a_0;a_1,\cdots,a_n]$，证明：$\frac{1}{\alpha}=[0;a_0,a_1,\cdots,a_n]$。

5. 证明：$\begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix}=\begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix}$。

6. 连分数 $\alpha^*=[a_n;\cdots,a_1]$ 称为连分数 $\alpha=[a_1;\cdots,a_n]$ 的对称分数。设 α^* 的各阶渐近分数为 $\alpha_k^*=\frac{p_k^*}{q_k^*}$，$k=1,2,\cdots,n$，$\alpha$ 的各阶渐近分数为 $\alpha_k=\frac{p_k}{q_k}$，$k=1,2,\cdots,n$。证明：$p_n^*=p_n$，$p_{n-1}^*=q_n$，$q_n^*=p_{n-1}$，$q_{n-1}^*=q_{n-1}$。

6.2　用连分数表示数

我们在第4章中已经讨论了如何用小数来表示实数。现在我们来考虑一个类似的问题，就是如何用连分数来表示实数。就像在用小数表示实数时那样，要想用连分数表示实数，必须先要解决两个问题。这两个问题是：用连分数表示实数的方法是否是唯一的？当连分数有无穷多个元素时，它的意义是什么？在什么条件下，一个无限连分数是有意义的。关于后一问题，我们在6.1中已经回答了一半，就是无限连分数的意义就是它的渐近分数的叙列的极限，但是我们还没有回答这一极限存在的条件是什么，以及我们主要讨论的简单无限连分数是否一定有意义。下面我们就来讨论这些问题。

定理6.2.1　每个简单连分数都表示一个实数。

证明　显然每个有限的简单连分数都表示一个有理数。因此我们只须证明每个简单无限连分数都有意义即可(其意义就是它的渐近分数的叙列的极限，因而是一个实数)。

设$[a_0;a_1,a_2,\cdots,a_n,\cdots]$是一个任意的简单无限连分数。$\alpha_0,\alpha_1,\cdots,\alpha_k,\cdots$是它的渐近分数。那么由引理6.1.2和定理6.1.2知

$$\frac{p_{n-1}}{q_{n-1}}-\frac{p_n}{q_n}=\frac{(-1)^n}{q_nq_{n-1}}$$

故在上式中令 $n=1$ 和 $n=2k$，那么由引理6.1.2(2)即得

$$\alpha_1>\alpha_3>\cdots>\alpha_{2n-1}>\cdots>\alpha_{2n}>\cdots\alpha_2>\alpha_0$$

而仍由$\frac{p_{n-1}}{q_{n-1}}-\frac{p_n}{q_n}=\frac{(-1)^n}{q_nq_{n-1}}$可知$|\alpha_{2n-1}-\alpha_{2n}|=\frac{1}{q_{2n-1}q_{2n}}\to 0$。故由区间套定理知$\alpha_0,\alpha_1,\cdots,\alpha_n,\cdots$存在极限$\alpha$,并且由区间套的形式和取极限的过程即可知

$$\alpha_1>\alpha_3>\cdots>\alpha_{2n-1}>\cdots>\alpha>\cdots>\alpha_{2n}>\cdots\alpha_2>\alpha_0$$

这就证明了定理。

下面给出一个无限简单连分数所代表的实数与此连分数的第n阶渐近分数之间的误差估计。

定理 6.2.2 设$\alpha=[a_0;a_1,\cdots,a_k,\cdots]$,其中$a_0$是任意整数,$a_i$,$i\geqslant 1$都是正整数,$\frac{p_k}{q_k}$是$\alpha$的第$k$阶渐近分数,则

(1) $\frac{1}{q_k(q_k+q_{k+1})}<\left|\alpha-\frac{p_k}{q_k}\right|<\frac{1}{q_kq_{k+1}}$, $k\geqslant 0$;

如果$\alpha=[a_0;a_1,\cdots,a_n]$,则上式对$0\leqslant k<n-1$成立;

(2) $\left|\alpha-\frac{p_{n+1}}{q_{n+1}}\right|<\left|\alpha-\frac{p_n}{q_n}\right|$。

证明 (1) 由引理 6.1.1 和定理 6.1.2 即得

$$\alpha=\frac{r_{k+1}p_k+p_{k-1}}{r_{k+1}q_k+q_{k-1}}$$

$$\alpha-\frac{p_k}{q_k}=\frac{r_{k+1}p_k+p_{k-1}}{r_{k+1}q_k+q_{k-1}}-\frac{p_k}{q_k}=\frac{(-1)^n}{q_k(r_{k+1}q_k+q_{k-1})}$$

但是由r_{k+1}的定义知$a_{k+1}<r_{k+1}<a_{k+1}+1$,故

$$\frac{1}{q_k((a_{k+1}+1)q_k+q_{k-1})}<\left|\alpha-\frac{p_k}{q_k}\right|<\frac{1}{q_k(a_{k+1}q_k+q_{k-1})}$$

因而由引理 6.1.3 就得出

$$\frac{1}{q_k(q_k+q_{k+1})}<\left|\alpha-\frac{p_k}{q_k}\right|<\frac{1}{q_kq_{k+1}}$$

(2) 由引理 6.1.3 得出

$$q_n(q_n+q_{n+1})<q_{n+1}(a_{n+2}q_{n+1}+q_n)=q_{n+1}q_{n+2}$$

因而由(1)已证的式子知

$$\left|\alpha-\frac{p_{n+1}}{q_{n+1}}\right|<\frac{1}{q_{n+1}q_{n+2}}<\frac{1}{q_n(q_n+q_{n+1})}<\left|\alpha-\frac{p_n}{q_n}\right|$$

上面这条定理表示,如果$\frac{p_k}{q_k}$是α的渐近分数,则α与$\frac{p_k}{q_k}$之间的误差必须满足某种约束。下面我们证明这一定理在某种意义下的逆命题,即如果一个分数与α之间的误差满足了某种约束,则此分数必是α的渐近分数。

定理 6.2.3 设$\left|\alpha-\frac{p}{q}\right|<\frac{1}{q^2}$,$\theta=|q^2\alpha-pq|$,$\frac{p}{q}=[a_0;a_2,\cdots,a_n]$,那

么$\frac{p}{q}$是α的渐近分数的充分必要条件是$\theta \leqslant \frac{q_n}{q_n+q_{n-1}}$。

证明　当$\alpha=\frac{p}{q}$时，$\frac{p}{q}$显然是α的渐近分数，这时$\theta=0<\frac{q_n}{q_n+q_{n-1}}$，反之如果$\theta<\frac{q_n}{q_n+q_{n-1}}$而$\theta=0$，则$\alpha=\frac{p}{q}$，因此$\frac{p}{q}$是$\alpha$的渐近分数。故以下不妨设$\theta>0$。

由$\left|\alpha-\frac{p}{q}\right|<\frac{1}{q^2}$得出$\theta<1$，因此$0<\theta<1$。

由于$\left|\alpha-\frac{p_n}{q_n}\right|=\frac{|q_n^2\alpha-p_nq_n|}{q_n^2}=\frac{\theta}{q_n^2}$，因此$\alpha-\frac{p_n}{q_n}=\pm\frac{\theta}{q_n^2}$。设$\epsilon$表示$+1$或者$-1$，那么取适当的$\epsilon$，可写$\alpha-\frac{p_n}{q_n}=\frac{\epsilon\theta}{q_n^2}$。又令$\alpha=\frac{p_n\beta+p_{n-1}}{q_n\beta+q_{n-1}}$，则

$$\frac{\epsilon\theta}{q_n^2}=\alpha-\frac{p_n}{q_n}=\frac{p_n\beta+p_{n-1}}{q_n\beta+q_{n-1}}-\frac{p_n}{q_n}=\frac{q_np_{n-1}-p_nq_{n-1}}{q_n(q_n\beta+q_{n-1})}=\frac{(-1)^n}{q_n(q_n\beta+q_{n-1})}$$

因此

$$\theta=\frac{q_n}{q_n\beta+q_{n-1}},\beta=\frac{q_n-\theta q_{n-1}}{\theta q_n}>\frac{\theta q_n-\theta q_{n-1}}{\theta q_n}=\frac{q_n-q_{n-1}}{q_n}>0$$

如果$\beta\geqslant 1$，则$\beta=\frac{q_n-\theta q_{n-1}}{\theta q_n}>1$，$q_n-\theta q_{n-1}\geqslant\theta q_n$，因此$\theta\leqslant\frac{q_n}{q_n+q_{n-1}}$；反之如果$\theta\leqslant\frac{q_n}{q_n+q_{n-1}}$，则从上式反推回去就得到$\beta\geqslant 1$，因此我们得出

$$\theta\leqslant\frac{q_n}{q_n+q_{n-1}}\Leftrightarrow\beta\geqslant 1$$

由

$$\alpha=\frac{p_n\beta+p_{n-1}}{q_n\beta+q_{n-1}}$$

得出

$$\alpha=[a_0;a_1,\cdots,a_n,\beta]$$

如果$\beta\geqslant 1$，则$\beta=[a_{n+1};a_{n+2},\cdots]$，$a_{n+1}>1$，而

$$\alpha=[a_0;a_1,\cdots,a_n,[a_{n+1};a_{n+2},\cdots]]=[a_0;a_1,\cdots,a_n,a_{n+1};a_{n+2},\cdots]$$

因此$[a_0;a_1,\cdots,a_n]=\frac{p_n}{q_n}=\frac{p}{q}$是$\alpha$的渐近分数。

如果$0<\beta<1$，则$\frac{1}{\beta}>1$，$a_n+\frac{1}{\beta}=2[a_n+c;a_{n+1},\cdots]$，$c\geqslant 1$，而

$$\alpha=[a_0;a_1,\cdots,a_{n-1},a_n,\beta]=[a_0;a_1,\cdots,a_{n-1},a_n+\frac{1}{\beta}]=$$
$$[a_0;a_1,\cdots,a_{n-1},[a_n+c;a_{n+1},\cdots]]=$$
$$[a_0;a_1,\cdots,a_{n-1},a_n+c,a_{n+1},\cdots]$$

故α的渐近分数为$\frac{p_0}{q_0},\frac{p_1}{q_1},\cdots,\frac{p_{n-1}}{q_{n-1}},\frac{p'_n}{q'_n},\frac{p_{n+1}}{q_{n+1}}$，其中

$$\frac{p'_n}{q'_n}=\frac{(a_n+c)p_{n-1}+p_{n-2}}{(a_n+c)q_{n-1}+q_{n-2}}=\frac{p_n+cp_{n-1}}{q_n+cq_{n-1}}$$

另外注意当 $k<n$ 时，$q_k<q_n$，当 $k\geqslant n$ 时，$q_k\geqslant q'_n>q_n$，因此对任意自然数 k，$q_n\neq q_k$，$q_n\neq q'_n$。由于 $\frac{p_0}{q_0},\frac{p_1}{q_1},\cdots,\frac{p_{n-1}}{q_{n-1}},\frac{p'_n}{q'_n},\frac{p_{n+1}}{q_{n+1}},\cdots$ 都是既约分数，故

$$\frac{p}{q}=\frac{p_n}{q_n}\neq\frac{p_k}{q_k},\frac{p}{q}=\frac{p_n}{q_n}\neq\frac{p'_n}{q'_n}$$

这就说明 $\frac{p}{q}$ 不可能是 α 的渐近分数。

综合上述证明就得到 $\frac{p}{q}$ 是 α 的渐近分数 $\Leftrightarrow\beta\geqslant1\Leftrightarrow\theta\leqslant\frac{q_n}{q_n+q_{n-1}}$。

利用上面的定理，我们可以得出一个更简明的判别法。

定理 6.2.4 如果 $\frac{p}{q}$，$q>0$ 满足 $\left|\alpha-\frac{p}{q}\right|\leqslant\frac{1}{2q^2}$，则 $\frac{p}{q}$ 必是 α 的渐近分数。

证明 由于 $\frac{q_n}{q_n+q_{n-1}}>\frac{q_n}{q_n+q_n}=\frac{1}{2}$，故由 $\left|\alpha-\frac{p}{q}\right|\leqslant\frac{1}{2q^2}$ 就得出

$$\theta=|q^2\alpha-pq|\leqslant\frac{1}{2}<\frac{q_n}{q_n+q_{n-1}}$$

其中 $\frac{p_n}{q_n}=\frac{p}{q}=[a_0;a_1,\cdots,a_n]$。因此由定理 6.2.3 就证明了 $\frac{p}{q}$ 必是 α 的渐近分数。

上面我们证明了每一个简单的（有限或无限）连分数都表示一个实数，下面我们证明其逆命题也是正确的，即

定理 6.2.5 每一个实数都可以表示成一个简单的（有限或无限）连分数。

证明 设 α 是一个实数，如果 α 是有理数，则 $\alpha=\frac{a}{b}$，$b>0$。由辗转相除法即得

$$\frac{a}{b}=q_0+\frac{r_0}{b},0<\frac{r_0}{b}<1$$

$$\frac{b}{r_0}=q_1+\frac{r_1}{r_0},0<\frac{r_1}{r_0}<1,q_1>1$$

$$\vdots$$

$$\frac{r_{n-3}}{r_{n-2}}=q_{n-1}+\frac{r_{n-1}}{r_{n-2}},0<\frac{r_{n-1}}{r_{n-2}}<1,q_{n-1}\geqslant1$$

$$\frac{r_{n-2}}{r_{n-1}}=q_n+\frac{r_n}{r_{n-1}},r_n=0,q_n>1$$

故 $\alpha=\frac{a}{b}=[q_0;q_1,\cdots,q_n]$，$q_n>1$，因此每一个有理数都可以表示成连分数。

如果 α 是无理数，则由 $\alpha=[\alpha]+\{\alpha\}$，$0<\{\alpha\}<1$ 即得

$$\alpha = a_0 + \frac{1}{\alpha_0}, a_0 = [\alpha], \alpha_0 = \frac{1}{\{\alpha\}} > 1$$

$$\alpha_0 = a_1 + \frac{1}{\alpha_1}, a_1 = [\alpha_0], \alpha_1 = \frac{1}{\{\alpha_0\}} > 1$$

$$\vdots$$

$$\alpha_{k-1} = a_k + \frac{1}{\alpha_k}, a_k = [\alpha_{k-1}], \alpha_k = \frac{1}{\{\alpha_{k-1}\}} > 1$$

$$\vdots$$

由定理6.2.2和定理6.1.3得

$$\left|\alpha - \frac{p_k}{q_k}\right| < \frac{1}{q_k q_{k+1}} < \frac{1}{q_k^2} < \frac{1}{(k-1)^2} \to 0$$

因此按照无限连分数的意义就有 $\alpha = [a_0; a_1, \cdots, a_k, \cdots]$，而由此连分数的构造过程显然可知这是一个简单连分数。这就证明了每一个无理数都可以表示成一个无限的简单连分数。

下面我们来讨论用连分数表示实数时，表示法的唯一性问题。

在用小数表示实数时，我们一开始并不能得出唯一性，这是因为在用有限小数表示实数时可以有两种表示方法(一种是有限形式的，另一种是无限形式的)，但是通过约定只用一种表示法，我们就可达到唯一性。类似的，在用有限连分数表示实数时，也可以有两种表示方法。即

$$[a_0; a_1, \cdots, a_n] = [a_0; a_1, \cdots, a_n - 1, 1]$$

但是显然在这所谓两种表示方法中的后者显得很没有"意思"，因此通过约定不用这种表示方法，我们就可达到唯一性。

约定 6.2.1 除非特别声明或在中间过程中(例如命题的证明过程中)，我们约定一个有限简单连分数的最后一个元素都是大于1的正整数。

在此约定下，我们就有

定理 6.2.6 每一个实数可用唯一的方式表示成有限或无限的简单连分数。

证明 设 α 是一个实数。如果 α 是有理数，则由定理6.2.5可知 α 可以表示成一个有限的简单连分数。并且由约定6.2.1知其最后一个元素都是大于1的正整数。

设 $A_n = [a_0; a_1, \cdots, a_n] = [b_0; b_1, \cdots, b_m] = B_m, a_n > 1, b_m > 1$。不妨设 $n \leq m$，我们对 n 用数学归纳法证明必有 $m = n, a_i = b_i, 0 \leq i \leq n$。

当 $n = 0$ 时，如果 $m \neq 0$，则 $m \geq 1$，那么由 $A_n = B_m$ 得出

$$A_0 = a_0 = [b_0; b_1, \cdots, b_m] = [b_0; [b_1, \cdots, b_m]] = b_0 + \frac{1}{[b_1, \cdots, b_m]}$$

由于 $m \geq 1, b_m > 1$，故 $[b_1; \cdots, b_m] > 1$(注意如果没有 $b_m > 1$ 这一约定，则有

可能$[b_1,\cdots,b_m]=1$)。由此得出上式左边是一个整数，而右边不是一个整数。这不可能，因此必然有 $m=0$，而这时由 $A_0=B_0$就得出 $a_0=b_0$，故当 $n=0$时，命题成立。

现在假设对于不大于 n 的自然数，命题成立。

如果 $A_{n+1}=[a_0;a_1,\cdots,a_{n+1}]=[b_0;b_1,\cdots,b_m]=B_m$，则由于 $m\geqslant n\geqslant 1$(一开始我们就假设了 $m\geqslant n$)，$a_{n+1}>1,b_m>1$，故

$$[a_1;a_2,\cdots,a_{n+1}]>1,[b_1;b_2,\cdots,b_m]>1$$

而
$$A_{n+1}=a_0+\frac{1}{[a_1;a_2,\cdots,a_{n+1}]}=b_0+\frac{1}{[b_1;b_2,\cdots,b_m]}=B_m$$

因此 $a_0=b_0$，因而

$$[a_1;a_2,\cdots,a_{n+1}]=[b_1;b_2,\cdots,b_m]$$

现在连分数$[a_1;a_2,\cdots,a_{n+1}]$分号后面的元素个数已是 n 个，因此由归纳法假设就得出 $m=n+1,a_i=b_i,1\leqslant i\leqslant n+1$。

这样由数学故纳法就证明了当 α 是有理数时，用有限简单连分数表示 α 的唯一性。

现在设 α 是无理数，于是由定理6.2.5知 α 可表示成为一个无限简单连分数

$$\alpha=[a_0;a_1,\cdots,a_n,\cdots]$$

如果 α 还有一个无限简单连分数表示$[b_0;b_1,\cdots,b_n,\cdots]$，那么

$$\alpha=[a_0;a_1,\cdots,a_n,\cdots]=[b_0;b_1,\cdots,b_n,\cdots]$$

对任意的 n，$\alpha=[a_0;a_1,\cdots,a_n,[a_{n+1};\cdots]]=[b_0;b_1,\cdots,b_n,[b_{n+1};\cdots]]$，由定理6.2.1知$[a_{n+1};\cdots]$和$[b_{n+1};\cdots]$分别表示两个实数 α' 和 β'，于是

$$\alpha=[a_0;a_1,\cdots,a_n,\alpha']=[b_0;b_1,\cdots,b_n,\beta']$$

由于

$$\alpha'=a_{n+1}+\frac{1}{\ddots}>1,\beta'=b_{n+1}+\frac{1}{\ddots}>1$$

故由上面已经证明的有限简单连分数表示的唯一性就得到

$$a_i=b_i,0\leqslant i\leqslant n,\alpha'=\beta'$$

由于 n 的任意性，我们就证明了用无限简单连分数表示无理数的唯一性。

注意：我们实际上证明了如果$[a_0;a_1,\cdots,a_{n-1},\zeta]=[b_0;b_1,\cdots,b_{m-1},\eta]$，其中 a_0,b_0 是任意整数，$a_i,1\leqslant i\leqslant n-1$ 和 $b_i,1\leqslant i\leqslant m-1$ 都是正整数，而 ζ,η 是大于1的任意实数，就必有 $m=n,a_i=b_i,0\leqslant i\leqslant n-1,\zeta=\eta$。这是比有限简单连分数的唯一性更强一点的命题。

习题6.2

1. 求以下无限简单连分数的值

(1) $[2;3,1,1,1,\cdots]$

(2) $[1;2,3,1,2,3,1,2,3,\cdots]$

(3) $[0;2,1,3,1,3,1,3,\cdots]$

(4) $[-2;2,1,2,1,2,1,\cdots]$

2. 求以下无理数的无限简单连分数，前 6 个渐进分数以及此无理数和它的前 6 个渐进分数的差的绝对值(用小数表示，精确到小数点后 12 位)。

(1) $\sqrt{7}$ (2) $\sqrt{13}$ (3) $\sqrt{29}$ (4) $\frac{\sqrt{10}+1}{3}$ (5) $\frac{5-\sqrt{37}}{3}$

3. 求$\sqrt[3]{2}$ 的无限简单连分数的前 6 个元素。

4. 设 a,b 是正整数，$a \mid b$，即 $b = ac$。证明：$[b;a,b,a,b,a,\cdots] = \frac{b+\sqrt{b^2+4c}}{2}$。

5. 设 $\alpha = [a_0;a_1,a_2,\cdots]$ 是一个无限简单连分数。证明：

(1) 当 $a_1 > 1$ 时，$-\alpha = [-a_0-1;1,a_1-1,a_2,a_3,\cdots]$；

(2) 当 $a_1 = 1$ 时，$-\alpha = [-a_0-1;a_2+1,a_3,\cdots]$。

6.3 二次无理数和循环连分数

当我们用小数表示实数时，我们已经知道一个有理数化成小数时一定是一个纯循环小数或者混循环小数，反过来一个纯循环小数或者混循环小数一定是一个有理数。而且我们也完全弄清了，在有理数中，在什么条件下，其小数表示是纯循环的。

因此自然发生这样的问题，即在用连分数表示数时，是否循环的连分数也完全刻画了某一类数的一种特征？如果是，那么在什么条件下，其连分数表示是纯循环的。下面我们就来介绍这方面的结果，总的结果是循环连分数完全刻画了实二次无理数的一种特征。

首先定义什么是二次无理数。

定义 6.3.1 无理的二次代数数称为是二次无理数，实的二次无理数称为实二次无理数。

引理 6.3.1

(1) α 是二次无理数的充分必要条件是$\alpha = r + s\sqrt{d}$，其中 r 和 s 是有理数，$s \neq 0$，d 是一个整数，且不是完全平方数；

(2) α 是实二次无理数的充分必要条件是$\alpha = r + s\sqrt{d}$，其中 r 和 s 是有理数，$s \neq 0$，$d > 0$ 是一个正整数，且不是完全平方数。

证明 (1) 设 α 是一个二次无理数，则存在整数 $a\neq 0,b,c$ 使 α 是整系数二次方程

$$ax^2+bx+c=0$$

的根。于是 $\alpha=r+s\sqrt{d}$，其中 $r=-\frac{b}{2a}$，$s=-\frac{1}{2a}$ 或 $\frac{1}{2a}$ 是有理数，显然 $s\neq 0$。$d=b^2-4ac$ 是整数，由于 α 是无理数，故 d 不是完全平方数。这就证明了必要性。

反过来，设 $\alpha=r+s\sqrt{d}$，其中 r 和 s 是有理数，$s\neq 0$，d 是一个整数，且不是完全平方数，于是 $\sqrt{d}$ 是无理数，因此 $\alpha=r+s\sqrt{d}$ 是无理数，否则由 $\sqrt{d}=\frac{\alpha-r}{s}$ 得出矛盾。

又由直接计算可知 α 是有理系数二次方程 $x^2-2rx+(r^2-ds^2)=0$ 的根，因此 α 是二次代数数，这就证明了充分性。

(2) 由 α 是实数和(1) 的证明类似可证。

定义 6.3.2 设 d 是一个整数，且不是完全平方数。称 $\alpha'=r-s\sqrt{d}$ 是 $\alpha=r+s\sqrt{d}$ 的共轭数(其中 r,s 是有理数)。

易于证明下面的引理：

引理 6.3.2 设 d 是一个整数，且不是完全平方数。r,s 是有理数，$\alpha=r+s\sqrt{d}\neq 0$，那么 $\alpha'=r-s\sqrt{d}\neq 0$。

引理 6.3.3 设 d 是一个整数，且不是完全平方数，那么

(1) 形如 $r+s\sqrt{d}$(其中 r,s 是有理数) 的数的和、差、积、商(除数不为零)仍是这种形式的数；

(2) 形如 $r+s\sqrt{d}$(其中 r,s 是有理数) 的数的和、差、积、商(除数不为零)的共轭数就等于这些数的共轭数的和、差、积、商。

引理 6.3.4 二次无理数 α 与其共轭数 α' 的和与积都是有理数，且当 $\alpha\neq 0$ 时，$\alpha\alpha'\neq 0$。

引理 6.3.5 设 α 是一个二次无理数，$ax^2+bx+c=0$ 是 α 所满足的二次方程，其中 a,b,c 都是整数，$a>0$，$(a,b,c)=1$，那么 α 所满足的二次方程是唯一的。

证明 设 α 满足两个整系数二次方程

$$g_1=a_1x^2+b_1x+c_1=0,a_1>0,(a_1,b_1,c_1)=1$$
$$g_2=a_2x^2+b_2x+c_2=0,a_2>0,(a_2,b_2,c_2)=1$$

则显然 α 也是 $a_2g_1-a_1g_2=(a_2b_1-a_1b_2)x+(a_2c_1-a_1c_2)=0$ 的根。

如果 $a_2b_1-a_1b_2\neq 0$，那么 $\alpha=-\frac{a_2c_1-a_1c_2}{a_2b_1-a_1b_2}$ 与 α 是无理数的假设矛盾。因此必有 $a_2b_1-a_1b_2=0$。那么这时

$$(a_2g_1 - a_1g_2)(\alpha) = a_2c_1 - a_1c_2 = 0$$

故

$$\frac{a_2}{a_1} = \frac{b_2}{b_1} = \frac{c_2}{c_1} = m > 0 \quad (\text{因为 } a_1 > 0, a_2 > 0)$$

再由 $1 = (a_2, b_2, c_2) = (ma_1, mb_1, mc_1) = m(a_1, b_1, c_1) = m$ 就得出 $a_2 = a_1, b_2 = b_1, c_2 = c_1$，故 α 所满足的二次方程是唯一的。

定义 6.3.3 称无限连分数 $\alpha = [a_0; a_1, a_2, \cdots]$ 是循环的，如果存在正整数 k 和 m 使得当 $n \geqslant m$ 时，总有 $a_{n+k} = a_n$，记为 $\alpha = [a_0; a_1, a_2, \cdots, a_{m-1}, \overline{a_m, a_{m+1}, \cdots, a_{m+k-1}}]$。如果可取 $m = 0$，则称 $\alpha = [a_0; a_1, a_2, \cdots]$ 是纯循环连分数。

定理 6.3.1 任何简单循环连分数表示一个实二次无理数，反之任何实二次无理数可用简单循环连分数表示。

证明 (1) 设 $\alpha = [a_0; a_1, a_2, \cdots, a_{m-1}, \overline{a_m, a_{m+1}, \cdots, a_{m+k-1}}]$，其中 a_0 是整数，$a_i, i \geqslant 1$ 是正整数。再设 $\beta = [\overline{a_m; a_{m+1}, \cdots, a_{m+k-1}}]$，则 $\beta = [a_m; a_{m+1}, \cdots, a_{m+k-1}, \beta]$，因此

$$\alpha = \frac{p_{m-1}\beta + p_{m-2}}{q_{m-1}\beta + q_{m-2}}, \beta = \frac{p_{m+k-1}\beta + p_{m+k-2}}{q_{m+k-1}\beta + q_{m+k-2}}$$

于是 β 满足整系数二次方程

$$q_{m+k-1}x^2 + (q_{m+k-2} - p_{m+k-1})x - p_{m+k-2} = 0$$

且显然它的二次项系数不为零。由 β 可表示成一个无限简单连分数可知，β 是一个无理数，因此 β 是一个实二次无理数。将 $\alpha = \frac{p_{m-1}\beta + p_{m-2}}{q_{m-1}\beta + q_{m-2}}$ 的分母有理化（即分子分母同乘以分母的共轭数）即得

$$\alpha = \frac{p_{m-1}\beta + p_{m-2}}{q_{m-1}\beta + q_{m-2}} = \frac{(p_{m-1}\beta + p_{m-2})(q_{m-1}\beta' + q_{m-2})}{s} = \frac{(-1)^m\beta + r}{s}$$

其中 r, s 都是有理数，且由于 α 的分母不为零，因此 $s \neq 0$。这就证明了 α 是一个实二次无理数。

(2) 反之设 α 是一个实二次无理数，则 α 可表示成一个无限简单连分数

$$\alpha = [a_0; a_1, a_2, \cdots] = [a_0; a_1, a_2, \cdots, a_{n-1}, r_n]$$

故

$$\alpha = \frac{p_{n-1}r_n + p_{n-2}}{q_{n-1}r_n + q_{n-2}}$$

由于 α 是实二次无理数，故 α 必满足一个二次项系数大于零的整系数既约二次方程

$$ax^2 + bx + c = 0, a > 0, (a, b, c) = 1$$

把 $\alpha = \frac{p_{n-1}r_n + p_{n-2}}{q_{n-1}r_n + q_{n-2}}$ 代入上式即得

$$A_n r_n^2 + B_n r_n + C_n = 0$$

其中

$$A_n = p_{n-1}^2 a + p_{n-1}q_{n-1}b + q_{n-1}^2 c$$

$$B_n = 2p_{n-1}p_{n-2}a + (p_{n-1}q_{n-2} + p_{n-2}q_{n-1})b + 2q_{n-1}q_{n-2}c$$

$$C_n = p_{n-2}^2 a + p_{n-2}q_{n-2}b + q_{n-2}^2 c$$

由直接计算得出

$$B_n^2 - 4A_nC_n = (b^2 - 4ac)(p_{n-1}q_{n-2} - p_{n-2}q_{n-1})^2 = b^2 - 4ac$$

这就是说方程 $A_n r_n^2 + B_n r_n + C_n = 0$ 的判别式不依赖于 n 或者说这个判别式对于所有的 n 都是不变的。再由定理 6.2.2 我们有

$$\left|\alpha - \frac{p_{n-1}}{q_{n-1}}\right| < \frac{1}{q_n q_{n-1}} < \frac{1}{q_{n-1}^2}$$

由此得出

$$p_{n-1} = \alpha q_{n-1} + \frac{\delta_{n-1}}{q_{n-1}}$$

其中
$$\delta_{n-1} = q_n(p_{n-1} - \alpha q_{n-1})$$

因而
$$|\delta_{n-1}| = |q_n(p_{n-1} - \alpha q_{n-1})| = q_{n-1}^2\left|\alpha - \frac{p_{n-1}}{q_{n-1}}\right| < 1$$

把上两个式子代入到 A_n 的表达式中，并利用 α 满足方程 $ax^2 + bx + c = 0$ 的条件就得到

$$A_n = a\left(\alpha q_{n-1} + \frac{\delta_{n-1}}{q_{n-1}}\right)^2 + b\left(\alpha q_{n-1} + \frac{\delta_{n-1}}{q_{n-1}}\right)q_{n-1} + cq_{n-1}^2 =$$

$$(a\alpha^2 + b\alpha + c)q_{n-1}^2 + 2a\alpha\delta_{n-1} + \frac{a\delta_{n-1}^2}{q_{n-1}^2} + b\delta_{n-1} =$$

$$2a\alpha\delta_{n-1} + \frac{q\delta_{n-1}^2}{q_{n-1}^2} + b\delta_{n-1}$$

由此得出

$$|A_n| < |2a\alpha| + |a| + |b|$$

同理(或由 $C_n = A_{n-1}$)

$$|C_n| < |2a\alpha| + |a| + |b|$$

再由 $B_n^2 = 4A_nC_n + b^2 - 4ac$ 可知 $|B_n|$ 也存在与 n 无关的上界。

于是当 $n \to \infty$ 时，A_n, B_n, C_n 都只能取有限个值(因为他们都是整数)，因而 r_n 也只能取有限个值，或者说集合 $\{r_n\}$ 必是一个有限集。因此必然存在一个下标 m 和一个整数 k 使得

$$r_m = r_{m+k}$$

这就证明了连分数 $\alpha = [a_0; a_1, a_2, \cdots]$ 必是循环的。

下面我们来弄清纯循环连分数代表什么样的二次无理数，或者说什么样的二次无理数可表示成纯循环连分数。为此我们需要先引进既约的二次无理数这一概念。

定义 6.3.4 实二次无理数 α 称为是既约的，如果 $\alpha > 1$，$-1 < \alpha' < 0$，其中 α' 表示 α 的共轭数。

定义 6.3.5 设 α 是实二次无理数，则称 α 所满足的既约整系数二次方程的判别式 D 为 α 的判别式，记为 $D(\alpha)$。

由引理6.3.1可知实二次无理数 α 一定可表示成 $\alpha = r + s\sqrt{d}$ 的形式，其中 r, s 是有理数，$s \neq 0$，$d > 0$ 是一个整数，且不是完全平方。下面给出实二次无理数的更确切的形式。

引理 6.3.6 所有判别式为 D 的实二次无理数可表为 $\frac{P+\sqrt{D}}{Q}$ 或 $\frac{P-\sqrt{D}}{Q}$ 的形式，其中 D 是一个正整数，且不是完全平方数，P 是一个整数，而 $Q > 0$ 是一个正整数。

证明 设 α 是一个实二次无理数，判别式为 D，则 α 必满足一个既约的整系数二次方程

$$ax^2 + bx + c = 0, a > 0, (a, b, c) = 1, D = b^2 - 4ac > 0$$

于是

$$\alpha = \frac{-b+\sqrt{D}}{2a} \text{或} \alpha = \frac{-b-\sqrt{D}}{2a}$$

由于 $2a > 0$ 和 b 都是整数，这就证明了引理。

下面给出 α 是即约的实二次无理数充分必要条件。

引理 6.3.7

(1) 设 $\alpha = r + s\sqrt{d}$，其中 r, s 是有理数，$s \neq 0$，$d > 0$ 是一个整数，且不是完全平方，那么 α 是既约二次无理数的充分必要条件是

$$0 < r < \max(r, 1-r) < s\sqrt{d} < 1 + r$$

(2) 设 α 是实二次无理数，判别式为 $D > 0$，其中 D 是一个正整数，且不是完全平方数。则 α 是既约的充分必要条件是 α 必可表为 $\frac{P+\sqrt{D}}{Q}$ 的形式，其中 P 是一个整数，而 $Q > 0$ 是一个正整数，且满足关系式

$$Q > 0, 0 < P < \sqrt{D}, \sqrt{D} - P < Q < \sqrt{D} + P < 2\sqrt{D}$$

证明 (1) 必要性：设 $\alpha = r + \sqrt{d}$ 是既约的，则

$$1 < r + s\sqrt{d}$$

$$-1 < r - s\sqrt{d} < 0$$

把上两式相加得出 $r > 0$，从上面的第二个式子得出 $r < s\sqrt{d} < r + 1$，从上面的第一个式子得出 $1 - r < s\sqrt{d}$，联合所得出的三个式子即得

$$0 < r < \max(r, 1-r) < s\sqrt{d} < 1 + r$$

必要性得证。

充分性：设 $0 < r < \max(r, 1-r) < s\sqrt{d} < 1 + r$，则由 $s\sqrt{d} < 1 - r$ 得出 $\alpha = r + s\sqrt{d} > 1$。由 $0 < r < s\sqrt{d} < 1 + r$ 得出 $-1 < r - s\sqrt{d} < 0$，即 $-1 < \alpha' < 0$，故 α 是既约的。充分性得证。

(2) 必要性：设 α 是既约的。由引理6.3.6知 α 必可表为 $\frac{P + \sqrt{D}}{Q}$ 或 $\frac{P - \sqrt{D}}{Q}$ 的形式。其中 D 是一个正整数，且不是完全平方数，P 是一个整数，而 $Q > 0$ 是一个正整数。如果 $\alpha = \frac{P - \sqrt{D}}{Q}$，则 $\alpha' = \frac{P + \sqrt{D}}{Q}$，于是由既约的定义可知 $\alpha' > \alpha > 1$，而这与 $-1 < \alpha' < 0$ 相矛盾，因此必须 $\alpha = \frac{P + \sqrt{D}}{Q}$，而 $\alpha' = \frac{P - \sqrt{D}}{Q}$。

令 $r = \frac{P}{Q}$，$s = \frac{1}{Q}$，那么由(1)已证明的结果可知

$$0 < r < s\sqrt{D}$$

$$1 - r < s\sqrt{D} < 1 + r$$

把 $r = \frac{P}{Q}$，$s = \frac{1}{Q}$ 代入上式，并经过整理和化简就得到

$$Q > 0, 0 < P < \sqrt{D}, \sqrt{D} - P < Q < \sqrt{D} + P < 2\sqrt{D}$$

充分性：设 $\alpha = \frac{P + \sqrt{D}}{Q}$，其中 P 是一个整数，而 $Q > 0$ 是一个正整数，且满足关系式

$$Q > 0, 0 < P < \sqrt{D}, \sqrt{D} - P < Q < \sqrt{D} + P < 2\sqrt{D}$$

那么令 $r = \frac{P}{Q}$，$s = \frac{1}{Q}$，则 $\alpha = r + s\sqrt{d}$，且根据必要性的证明中关于不等式的转化部分知

$$0 < r < s\sqrt{D}$$

$$1 - r < s\sqrt{D} < 1 + r$$

因此
$$0 < r < \max(r, 1-r) < s\sqrt{d} < 1 + r$$

因而由(1)已证明的结果即得 α 是既约的。

下面我们再证明，对每一个不是完全平方数的正整数 d，都至少存在一个形如 $r + s\sqrt{d}$ 既约的实二次无理数。

引理6.3.8 设 d 是正整数，且不是完全平方数，则至少存在一个形如 $r + s\sqrt{d}$ 的既约实二次实无理数，其中 r, s 是有理数，$s \neq 0$。

证明 由 d 是正的非完全平方数知 $d>1$，故 $\sqrt{d}>1$，$r=[\sqrt{d}]>1$。由 r 的定义知

$$0<r<\sqrt{d}<1+r$$

令 $\alpha=r+\sqrt{d}$，则 $\alpha>r>1$。同时 $-1<r-\sqrt{d}<0$，即 $-1<\alpha'<0$。因此 $\alpha=r+\sqrt{d}$ 就是一个形如 $r+s\sqrt{d}$ 的既约实二次实无理数。

下面来研究既约实二次无理数有什么性质。

引理 6.3.9 设 α 是一个实二次无理数，a_1 是一个整数。

$$\alpha=a_1+\frac{1}{\beta}$$

则 β 也是一个实二次无理数，且 α 和 β 所满足的既约整系数二次方程(即方程的各项系数的最大公因数为 1) 的判别式相同。

证明 由 $\beta=\dfrac{1}{\alpha-a_1}$ 首先知道 β 是无理数。再由引理 6.3.1 和引理 6.3.3 就知道 β 也是实二次无理数。现设 α 满足既约整系数二次方程

$$ax^2+bx+c=0,(a,b,c)=1$$

则对此方程两边取共轭可知它的另一个根是 α'，故由根与系数的关系得出

$$\alpha+\alpha'=-\frac{b}{2a},\alpha\alpha'=\frac{c}{a}$$

由 $\beta=\dfrac{1}{\alpha-a_1}$ 得出 $\beta'=\dfrac{1}{\alpha'-a_1}$，由此通过直接计算可以得出

$$\beta+\beta'=-\frac{2aa_1+b}{aa_1^2+ba_1+c}$$

$$\beta\beta'=\frac{a}{aa_1^2+ba_1+c}$$

故再由根与系数的关系得知 β 满足整系数二次方程

$$(aa_1^2+ba_1+c)x^2+(2aa_1+b)x+a=0$$

易证 $m\mid(aa_1^2+ba_1+c,2aa_1+b,a)$ 蕴含 $m\mid(a,b,c)$。因此由 $(a,b,c)=1$ 显然就得出 $(aa_1^2+ba_1+c,2aa_1+b,a)=1$。这就是说方程 $(aa_1^2+ba_1+c)x^2+(2aa_1+b)x+a$ 已是既约的。通过直接计算得出此方程的判别式为

$$D_2=(2aa_1+b)^2-4a(aa_1^2+ba_1+c)=b^2-4ac$$

故方程 $(aa_1^2+ba_1+c)x^2+(2aa_1+b)x+a=0$ 的判别式就是方程 $ax^2+bx+c=0$ 的判别式，这就证明了引理。

引理 6.3.10 设 α 是一个既约的实二次无理数，$a_1=[\alpha]$，$\alpha=a_1+\dfrac{1}{\beta}$，则

β 也是一个既约的实二次无理数。

证明 由引理6.3.9即知 β 也是实二次无理数。

从 α 既约得出 $\alpha > 1$，故 $a_1 = [\alpha] > 1$。且由 a_1 的定义知 $1 < a_1 < \alpha < a_1 + 1$，故 $0 < \alpha - a_1 < 1$，因此 $\beta = \frac{1}{\alpha - a_1} > 1$。

从 α 既约又得出 $-1 < \alpha' < 0$，再由 $a_1 = [\alpha] > 1$ 就得出 $-1 - a_1 < \alpha' - a_1 < -a_1 < -1$，所以

$$-1 < -\frac{1}{a_1} < \frac{1}{\alpha' - a_1} < -\frac{1}{1 + a_1} < 0$$

但是 $\beta' = \frac{1}{\alpha' - a_1}$，所以上式就是 $-1 < \beta' < 0$。这就证明了 β 也是既约的。

引理6.3.11 设 α 是一个既约的实二次无理数，则 $\beta = -\frac{1}{\alpha'}$ 也是既约的实二次无理数。

证明 由 α' 的定义和引理6.3.1和引理6.3.3易证 β 也是实二次无理数。

从 α 既约得出 $-1 < \alpha' < 0$，故 $0 < \alpha' < -1$。由此得出 $\beta = -\frac{1}{\alpha'} > 1$。又在 $\beta = -\frac{1}{\alpha'}$ 两边取共轭得出 $\beta' = -\frac{1}{\alpha}$，从而由 α 既约得出 $\alpha > 1$，$-1 < -\frac{1}{\alpha} < 0$，这就是 $-1 < \beta' < 0$。这就证明了 β 也是既约的。

引理6.3.12 设 $D > 0$，其中 D 是一个正整数，且不是完全平方数，那么以 D 为判别式的既约实二次无理数的个数是有限的。

证明 设 α 是以 D 为判别式的既约的实二次无理数。则由引理6.3.7知 α 必可表为 $\frac{P + \sqrt{D}}{Q}$ 的形式，其中 P 是一个整数，而 $Q > 0$ 是一个正整数，且满足关系式

$$Q > 0, 0 < P < \sqrt{D}, \sqrt{D} - P < Q < \sqrt{D} + P < 2\sqrt{D}$$

由 $0 < P < \sqrt{D}$ 及 P 是整数知 P 的个数是有限的，再由 $0 < Q < 2\sqrt{D}$ 知 Q 的个数也是有限的。故所有形如 $\frac{P + \sqrt{D}}{Q}$，$Q > 0$ 的数的个数也是有限的，这就证明了引理。

上面讲了这么多关于既约实二次无理数的性质，有的是为了给下面的内容作准备，有的是既然谈到这个既约问题，就把有关的事实放在一起介绍一下。下面就可以给出这一节中后半部分的主要结果了。这就是

定理6.3.2 循环节元素为正整数的纯循环连分数是一个既约的实二次无理数。

证明 设 $\alpha = [\overline{a_1; a_2, \cdots, a_n}]$，其中 $a_i (1 \leqslant i \leqslant n)$ 为正整数，$\beta = [\overline{a_n; a_{n-1}, \cdots, a_1}]$。

$$[a_1;a_2,\cdots,a_{n-1}]=\frac{p_{n-1}}{q_{n-1}},[a_1;a_2,\cdots,a_n]=\frac{p_n}{q_n}$$

$$[a_n;a_{n-1},\cdots,a_2]=\frac{p'_{n-1}}{q'_{n-1}},[a_n;a_{n-1},\cdots,a_1]=\frac{p'_n}{q'_n}$$

则由定理 6.1.1 可知

$$\alpha=[a_1;a_2,\cdots,a_n,\alpha]=\frac{p_n\alpha+p_{n-1}}{q_n\alpha+q_{n-1}}$$

$$\beta=[a_n;a_2,\cdots,a_1,\beta]=\frac{p'_n\beta+p'_{n-1}}{q'_n\beta+q'_{n-1}}=\frac{p_n\beta+q_n}{p_{n-1}\beta+q_{n-1}}$$

由此可知 α 满足整系数二次方程

$$q_nx^2-(p_n-q_{n-1})x-p_{n-1}=0$$

而 β 满足整系数二次方程

$$p_{n-1}x^2-(p_n-q_{n-1})x-q_n=0$$

由此易于验证 $-\frac{1}{\beta}$ 是α所满足的整系数二次方程的另一个根。显然 α 和β都是无理数(否则表示它们的连分数将是有限的而不可能是循环的)。而由实二次无理数的共轭数的定义可知 $\alpha'=-\frac{1}{\beta}$。由 α 和β 的定义又可知

$$\alpha=[a_1;r_1]>a_1\geqslant 1$$

同理 $\beta>1$,因此有

$$\alpha>1,-1<\alpha'=-\frac{1}{\beta}<0$$

这就证明了 α 是既约的实二次无理数。

下面我们来证明这一定理的逆定理也成立。

定理 6.3.3　既约的实二次无理数必可表示为一个元素都是正整数的纯循环连分数。

证明　设α是一个既约的实二次无理数,则 $\alpha>1$,因此 $a_1=[\alpha]>1$。令 $\alpha=a_1+\frac{1}{\alpha_1}$,则由引理 6.3.11 知 α_1 也是既约的实二次无理数。再令 $a_2=[\alpha_1]$, $\alpha_1=a_2+\frac{1}{\alpha_2}$,则同理可知 $a_2\geqslant 1$,α_2是既约的实二次无理数。由于 α 是无理数,所以这一过程可无限进行下去,故

$$\alpha=[a_1;a_2,\cdots,a_n,\cdots]$$

其中 $a_1,a_2,\cdots,a_n,\cdots$ 都是正整数。

由引理 6.3.9 知,实二次无理数 $\alpha,\alpha_1,\cdots,\alpha_n,\cdots$ 具有相同的判别式 $D(\alpha)$,而由引理 6.3.12 知,以 $D(\alpha)$ 为判别式的既约的实二次无理数只有有限多个。因此由 $\alpha,\alpha_1,\cdots,\alpha_n$ 都是既约的实二次无理数便得出集合$\{\alpha,\alpha_1,\cdots,\alpha_n\}$ 是一

个有限集。因此必然存在下标 m 和 k 使得 $\alpha_m = \alpha_k$。不妨设 m 是这种下标中的最小者，α_k 是叙列 $\alpha,\alpha_1,\cdots,\alpha_n,\cdots$ 中第一个与 α_m 重合者。于是 $\alpha,\alpha_1,\cdots,\alpha_{m-1}$ 都不相同，而 $\alpha_m = \alpha_k$。由于

$$\alpha_k = a_{k+1} + \frac{1}{\alpha_{k+1}},\alpha_m = a_{m+1} + \frac{1}{\alpha_{m+1}}$$

而

$$a_{k+1} = [\alpha_k] = [\alpha_m] = a_{m+1}$$

所以

$$\alpha_{k+1} = \frac{1}{\alpha_k - a_{k+1}} = \frac{1}{\alpha_m - a_{m+1}} = \alpha_{m+1}$$

依次类推即得

$$\alpha_{k+1} = \alpha_{m+1},\alpha_{k+2} = \alpha_{m+2},\alpha_{k+3} = \alpha_{m+3},\cdots$$

这就是说，叙列 $\alpha,\alpha_1,\cdots,\alpha_n,\cdots$ 从 α_m 起开始循环。

又由 $\alpha_k = \alpha_m$ 得出

$$\alpha'_k = \alpha'_m,\beta_k = -\frac{1}{\alpha'_k} = -\frac{1}{\alpha'_m} = \beta_m$$

而

$$\alpha_{k-1} = a_k + \frac{1}{\alpha_k},\alpha_{m-1} = a_m + \frac{1}{\alpha_m}$$

故

$$\alpha'_{k-1} = a_k + \frac{1}{\alpha'_k},\alpha'_{m-1} = a_m + \frac{1}{\alpha'_m}$$

因此

$$-\frac{1}{\beta_{k-1}} = a_k - \beta_k,-\frac{1}{\beta_{m-1}} = a_m - \beta_m$$

或者

$$\beta_k = a_k + \frac{1}{\beta_{k-1}},\beta_m = a_m + \frac{1}{\beta_{m-1}}$$

由于 α_{k-1} 和 α_{m-1} 都是既约的，故 $-1 < \alpha'_{k-1} < 0,-1 < \alpha'_{m-1} < 0$，这也就是

$$0 < -\alpha'_{k-1} = \frac{1}{\beta_{k-1}} < 1,0 < -\alpha'_{m-1} = \frac{1}{\beta_{m-1}} < 1$$

$\beta_k = a_k + \frac{1}{\beta_{k-1}}$ 和 $0 < \frac{1}{\beta_{k-1}} < 1$ 说明 $[\beta_k] = a_k$，同理 $[\beta_m] = a_m$。再由已证的 $\beta_k = \beta_m$ 即得

$$a_k = [\beta_k] = [\beta_m] = a_m$$

再由 $a_k = a_m$ 和 $\alpha_{k-1} = a_k + \frac{1}{\alpha_k},\alpha_{m-1} = a_m + \frac{1}{\alpha_m}$ 即得出 $\alpha_{k-1} = \alpha_{m-1}$。依次类推就得出

$$\alpha_k = \alpha_m,\alpha_{k-1} = \alpha_{m-1},\alpha_{k-2} = \alpha_{m-2},\cdots,\alpha_{k-m} = \alpha$$

令 $k - m = s$，那么从上式和 $\alpha_{k+1} = \alpha_{m+1},\alpha_{k+2} = \alpha_{m+2},\alpha_{k+3} = \alpha_{m+3},\cdots$ 可知 α，$\alpha_1,\cdots,\alpha_{s-1}$ 两两不同，而 $\alpha_s = \alpha$，并从此后开始循环。而由 $a_i = [\alpha_i]$ 知叙列 a_1，$a_2,\cdots,a_s$ 也将重复循环，也就是说由于

$$\alpha_s = a_{s+1} + \frac{1}{\alpha_{s+1}} = \alpha = a_1 + \frac{1}{\alpha_1}$$

我们将得出

$$a_{s+1} = a_1, a_{s+2} = a_2, \cdots$$

这就证明了 $\alpha = [\overline{a_1; a_2, \cdots, a_s}]$，也就是说，$\alpha$ 可表示成元素都是正整数的纯循环连分数。

现在我们引入循环连分数的周期这一概念。

定义 6.3.6 设 $\alpha = [a_0; a_1, a_2, \cdots]$ 是循环连分数，因此存在正整数 k 和 m 使得当 $n \geqslant m$ 时，总有 $a_{n+k} = a_n$，则称使等式 $a_{n+k} = a_n$ 成立的最小正整数为此循环连分数的周期。

下面的定理给出了周期的性质。

定理 6.3.4 设 $\alpha = [a_0; a_1, a_2, \cdots]$，$r_n = [a_n; a_{n+1}, a_{n+2}, \cdots]$，那么

(1) α 是纯循环连分数的充分必要条件是存在整数 k，使 $\alpha = r_k$；

(2) α 是周期为 l 的纯循环连分数的充分必要条件是 $l \mid k$，其中整数 k 使得 $\alpha = r_k$；

(3) 设 α 是纯循环连分数，那么对于任意的 $n > 0$，r_n 也是纯循环连分数，而且周期相同。

证明 (1) 设 α 是纯循环连分数，那么由纯循环连分数的定义就得出 $\alpha = r_k$。反之如果 $\alpha = r_k$，则

$$\alpha = [a_0; a_1, \cdots, a_{k-1}, r_k] = [a_0; a_1, \cdots, a_{k-1}, \alpha] = [\overline{a_0; a_1, \cdots, a_{k-1}}]$$

因此 α 是纯循环连分数。

(2) α 是周期为 l 的纯循环连分数，$\alpha = r_k$，则对任意的 $n \geqslant 0$ 成立 $a_{n+k} = a_n$。由周期的极小性就推出 $l \leqslant k$，因而由带余数除法可知 $k = ql + r, q \geqslant 0, 0 \leqslant r < l$。再由 l 表示 α 的周期可知对任意 $n \geqslant 0$ 有 $a_n = a_{n+k} = a_{n+r+ql} = a_{n+r}$，这说明 r 也是 α 的周期，因而由周期的极小性就得出 $r = 0$，即 $l \mid k$。

反之，如果 $l \mid k$，则由周期的定义就得出对任意的 $n \geqslant 0$ 成立 $a_{n+k} = a_{n+ql} = a_n$，因此 α 是纯循环的，且 $\alpha = r_k$。

(3) 设 α 是纯循环的，则由纯循环连分式的表示式即知对任意的 $n > 0$，r_n 也是纯循环的，且其循环节仅是 α 的循环节的某种轮换，因而 r_n 与 α 有相同的周期。

至此，就像我们已搞清了每一个循环小数都表示一个有理数，而每一个纯循环小数则表示一个分母中不含因子 2 和 5 的既约分数一样，并且反过来也对。我们也搞清了每一个循环连分数都表示一个实二次无理数，而每一个纯循环连分数则表示一个既约的实二次无理数，并且反过来也对。

而遗留下来的问题有，对于更高次的无理代数数，乃至超越数，我们是否也能得出它们的某种特性。

习题 6.3

1. 求以下实二次无理数的循环连分数表示式，它的纯循环部分和周期

(1) $\frac{5+\sqrt{37}}{}$　　(2) $\sqrt{43}$　　(3) $\frac{6+\sqrt{43}}{7}$

(4) $8+\sqrt{80}$　　(5) $\frac{3+\sqrt{7}}{2}$　　(6) $\sqrt{\frac{26}{5}}$

2. 设 $\alpha=[\overline{a_0;a_1,\cdots,a_n}]$，$\alpha'$ 表示 α 的共轭数。证明：$-\frac{1}{\alpha}=[\overline{a_n;a_{n-1},\cdots,a_0}]$。

3. 证明：$\sqrt{d}$ 的循环连分数的周期为 1 的充分必要条件是 $d=a^2+1$（a 是正整数），且 $\sqrt{a^2+1}=[a;\overline{2a}]$，由此求出 $\sqrt{101}$，$\sqrt{325}$ 和 $\sqrt{2\,602}$ 的循环连分数。

4. 设整数 $a\geqslant 2$，证明：

(1) $\sqrt{a^2-1}=[a-1;\overline{1,2a-2}]$；

(2) $\sqrt{a^2-a}=[a-1;\overline{2,2a-2}]$。

利用上述结果给出一些应用。

5. 设整数 $a\geqslant 3$，证明：

(1) $\sqrt{a^2-2}=[a-1;\overline{1,a-2,1,2a-2}]$；

(2) $\sqrt{a^2+2}=[a;\overline{a,2a}]$。

利用上述结果给出一些应用。

6. 设 a 是奇数，证明：

(1) 当 $a>1$ 时，$\sqrt{a^2+4}=[a;\overline{\frac{a-1}{2},1,1,\frac{a-1}{2},2a}]$；

(2) 当 $a>3$ 时，$\sqrt{a^2-4}=[a-1;\overline{1,\frac{a-3}{2},2,\frac{a-3}{2},1,2a-2}]$。

利用上述结果给出一些应用。

7. 证明：$\sqrt{d}$ 的循环连分数的周期为 2 的充分必要条件是 $d=a^2+b$，$b>1$，$b\mid 2a$（a,b 是正整数），且 $\sqrt{a^2+b}=[a;\overline{\frac{2a}{b},2a}]$。利用此结果给出一些应用。

8. 求出所有形如 $\frac{P+\sqrt{43}}{Q}$ 的既约实二次无理数。

9. 设 $\alpha=[a_0,a_1,a_2,\cdots,a_n,\cdots]$ 是一个实二次无理数，其中 a_0 是整数，

$a_i(i \geqslant 1)$ 都是正整数。它所满足的既约整系数二次方程的两个根为 α 和 β。证明:

(1) 如果 $\alpha = [\overline{a_1; a_2, \cdots, a_n}]$,则 $-1 < \beta < 0$;

(2) 如果 $\alpha = [a_0; \overline{a_1, a_2, \cdots, a_n}]$,则 $\beta < -1$ 或者 $\beta > 0$;

(3) 如果 α 的非循环部分至少含有两个元素,例如 $\alpha = [a_0; a_1, \overline{a_2, a_3, \cdots, a_n}]$,则 $\beta > 0$。

6.4 连分数的应用 Ⅰ:集合论中的一个定理

在第 2 章 2.3 中,我们曾经证明过一个定理:

定理 2.3.6 设 A 中的每一个元素都有有限个互相独立的下标,每一个下标可以是任意的自然数,则 A 是至多可数集。

这也就是说如果 $A = \{a_{n_1, n_2, \cdots n_k} \mid$ 其中 $n_1, n_2, \cdots, n_k$ 都是自然数,n_i 的个数 k 依赖于 $a\}$,则 A 是至多可数的。

这里我们要特别指出一点值得注意的地方,那就是虽然上述定理中 A 中元素的下标的个数可以是任意的,而且对于 A 中不同的元素,下标的个数还可以不同。但是却必须每一次只用有限个下标,而不能出现无限多个下标。

但是在有些问题中,集合中的元素却需要用无限多个自然数加以描述。现在我们就来研究一下这种集合的势。

定理 6.4.1(定理 2.4.6) 设 $Q = \{(n_1, n_2, n_3, \cdots) \mid n_1, n_2, n_3, \cdots$ 都是自然数$\}$,则 Q 的势是 c。

证明 令 Q 中的元素$(n_1, n_2, n_3, \cdots)$和$(0,1)$中的无理数 $\alpha = [0; n_1, n_2, n_3, \cdots]$ 相对应,由无限连分数表示法的唯一性可知 Q 与$(0,1)$中的无理数是 1—1 对应的,但是$(0,1)$中全体无理数组成的集合的势显然是 c,这就证明了定理。

你看,用连分数理论来证明这一定理是多么简单。数学中常常就有这种事,就是不同问题所引起的研究,常常会意想不到地对解决其他的问题发生作用。比如康托从研究集合问题开始所导致的集合论却无意中可以得出无理数乃至超越数的存在性,现在我们又从连分数的研究无意中获得了集合论中定理的证明。

6.5 连分数的应用 Ⅱ：不定方程 $ax \pm by = c$ 的特解

在第3章3.5中我们已经弄清了二元一次不定方程 $ax+by=c$ 有解的条件，并且知道在它有解时如果已知不定方程 $ax+by=c$ 的一组特解 x_0, y_0，那么它的所有解就可以写成 $x=x_0-bt, y=y_0+at$ 或 $x=x_0+bt, y=y_0-at$ 的形式。并且指出，可以用辗转相除法来求出这组特解。

当不定方程 $ax+by=c$ 有解时，我们只须求出不定方程 $ax+by=1$ 的解，那么只要把后者的解乘以 c 就可得到前者的解。因此最后全部的问题就归结为求出不定方程 $ax+by=1$ 的特解。

现在我们要问，是否能用一个明确的公式来给出这组特解。

定理6.5.1 设 $(a,b)=1, a>0, b>0$。$\frac{a}{b}=[a_0;a_1,\cdots,a_n]$，$\frac{p_k}{q_k}$ 是 $\frac{a}{b}$ 的第 k 阶渐近分数，那么不定方程

(1) $ax+by=1$ 的一组特解是 $x_0=(-1)^{n-1}q_{n-1}, y_0=(-1)^n p_{n-1}$；

(2) $ax-by=1$ 的一组特解是 $x_0=(-1)^{n-1}q_{n-1}, y_0=(-1)^{n-1}p_{n-1}$；

(3) $ax+by=-1$ 的一组特解是 $x_0=(-1)^n q_{n-1}, y_0=(-1)^{n-1}p_{n-1}$；

(4) $ax-by=-1$ 的一组特解是 $x_0=(-1)^n q_{n-1}, y_0=(-1)^n p_{n-1}$。

证明 由定理6.1.2知

$$q_n p_{n-1}-p_n q_{n-1}=(-1)^n$$

故 $(p_n,q_n)=(a,b)=1$，又由渐近分数的定义知 $\frac{p_n}{q_n}=\frac{a}{b}$，所以 $p_n=a, q_n=b$，由此得出

$$bp_{n-1}-aq_{n-1}=(-1)^n$$
$$aq_{n-1}-bp_{n-1}=(-1)^{n+1}$$

由上式就不难看出上面四种不定方程的特解。

在应用上面这个定理时，我们不必死记硬背定理中的公式而只须注意到上面四种不定方程都可化为统一的形式

$$ax+by=1$$

这里 a, b 可以是任意整数，然后设 $\frac{|a|}{|b|}=[a_0;a_1,a_2,\cdots,a_n]$，而 $\frac{p_{n-1}}{q_{n-1}}$ 是此连分数的倒数第2阶的渐近分数，那么 (q_{n-1},p_{n-1})，$(q_{n-1},-p_{n-1})$，$(-q_{n-1},p_{n-1})$，$(-q_{n-1},-p_{n-1})$ 这四组解中，或由正负号搭配而成的四组解 $(\pm q_{n-1}, \pm p_{n-1})$

中必有一组是 $ax+by=1$ 的特解就很容易记住这一公式了。

6.6 连分数的应用 Ⅲ:Pell 方程

不定方程

$$x^2-dy^2=1$$

和不定方程

$$x^2-dy^2=-1$$

都称为 Pell 方程,其中 $d>0$ 是一个正整数,且不是完全平方数。显然 $x=1$,$y=0$ 是方程 $x^2-dy^2=1$ 的一组解,我们称这组解为平凡解。我们的问题和兴趣在于求出 Pell 方程的非平凡解。今后可以证明方程 $x^2-dy^2=1$ 必有非平凡解存在,而方程 $x^2-dy^2=-1$ 却不一定。因此我们的课题就是对方程 $x^2-dy^2=1$ 和方程 $x^2-dy^2=-1$ 给出非平凡解存在的条件,并且在它们存在非平凡解时,求出它们的全部非平凡解。

在解决二元一次不定方程时,我们已经知道,特解起了非常重大的作用,这就是说,如果知道了不定方程 $ax+by=c$ 的一组特解 x_0,y_0,那么就可以求出这个不定方程的所有解。

在解 Pell 方程时,特解同样起着非常重要的作用,这一回,虽然我们不能说知道了 Pell 方程的一组特解就可以求出它的所有解,但是起码可以说,知道了一组特解,就可以求出它的无穷多组解来。

引理 6.6.1 设 $d>0$ 是一个正整数,且不是完全平方数,又设 x_1,x_2,y_1,y_2 都是整数,则

$$x_1+y_1\sqrt{d}=x_2+y_2\sqrt{d}$$

的充分必要条件是

$$x_1=x_2,y_1=y_2$$

证明 如果 $x_1=x_2,y_1=y_2$,那么显然

$$x_1+y_1\sqrt{d}=x_2+y_2\sqrt{d}$$

反之,设 $x_1+y_1\sqrt{d}=x_2+y_2\sqrt{d}$,如果 $y_1\neq y_2$,那么

$$\sqrt{d}=\frac{x_1-x_2}{y_2-y_1}$$

由于上式左边是一个无理数,而右边是一个有理数,因此上式显然不可能成立。这就说明,必须有 $y_1=y_2$,从而 $x_1=x_2$。

引理 6.6.2 设 $d>0,x_1,x_2,y_1,y_2$ 都是整数,则

$$(x_1^2-dy_1^2)(x_2^2-dy_2^2)=(x_1x_2+dy_1y_2)^2-d(x_1y_2+x_2y_1)^2$$

证明　用乘法直接验证即可。

定义 6.6.1　设 $d>0$ 是一个正整数，且不是完全平方数。则当且仅当 x_0，y_0 是方程 $x^2-dy^2=-1$ 或方程 $x^2-dy^2=-1$ 的一组非平凡解时，称 $\alpha=x_0+y_0\sqrt{d}$ 给出方程 $x^2-dy^2=1$ 或方程 $x^2-dy^2=-1$ 的一组解。

引理 6.6.3

(1) 如果 α 给出方程 $x^2-dy^2=1$ 的一组解，则 $-\alpha,\alpha',\frac{1}{\alpha}$ 分别给出它的另一组解；

(2) 如果 α 给出方程 $x^2-dy^2=-1$ 的一组解，则 $-\alpha,\alpha',\frac{1}{\alpha}$ 分别给出它的的另一组解。

证明　(1) 设 $\alpha=x_0+y_0\sqrt{d}$ 给出方程 $x^2-dy^2=1$ 的一组解。

那么 $-\alpha=-x_0-y_0\sqrt{d}$，$\alpha'=x_0-y_0\sqrt{d}$，由此显然就立刻得出 $-\alpha,\alpha'$ 分别给出它的另一组解

$$\frac{1}{\alpha}=\frac{x_0^2-dy_0^2}{x_0+y_0\sqrt{d}}=x_0-y_0\sqrt{d}=\alpha'$$

因此 $\frac{1}{\alpha}$ 给出方程 $x^2-dy^2=1$ 的另一组解。

(2) 设 $\alpha=x_0+y_0\sqrt{d}$ 给出方程 $x^2-dy^2=-1$ 的一组解。

那么 $-\alpha=-x_0-y_0\sqrt{d}$，$\alpha'=x_0-y_0\sqrt{d}$，由此显然就立刻得出 $-\alpha,\alpha'$，分别给出它的另一组解

$$\frac{1}{\alpha}=-\frac{x_0^2-dy_0^2}{x_0+y_0\sqrt{d}}=-(x_0-y_0\sqrt{d})=-\alpha'$$

因此 $\frac{1}{\alpha}$ 给出方程 $x^2-dy^2=-1$ 的另一组解。

由引理6.6.3可知，只要求出了 Pell 方程的所有正的非平凡解，那么就可知道 Pell 方程的所有非平凡解了，因此以下我们只考虑 Pell 方程的正的非平凡解。当我们再说到非平凡解时，也都指正的非平凡解。

引理 6.6.4

(1) 如果 α_1,α_2 给出方程 $x^2-dy^2=1$ 的解，则 $\alpha_1\alpha_2$ 也给出它的解；

(2) 如果 $\alpha_1,\alpha_2,\alpha_3$ 给出方程 $x^2-dy^2=-1$ 的解，则 $\alpha_1\alpha_2$ 给出方程 $x^2-dy^2=1$ 的解，$\alpha_1\alpha_2\alpha_3$ 给出方程 $x^2-dy^2=-1$ 的解。

证明　(1) 设 $\alpha_1=x_1+y_1\sqrt{d}$，$\alpha_2=x_2+y_2\sqrt{d}$ 给出方程 $x^2-dy^2=1$ 的解，则

$$\alpha_1\alpha_2 = (x_1x_2 + dy_1y_2) + (x_1y_2 + x_2y_1)\sqrt{d}$$

而由引理 6.6.2,我们有

$$(x_1x_2 + dy_1y_2)^2 - d(x_1y_2 + x_2y_1)^2 = (x_1^2 - dy_1^2)(x_2^2 - dy_2^2) = 1$$

这就说明 $\alpha_1\alpha_2$ 也给出方程 $x^2 - dy^2 = 1$ 的解。

(2) 设 $\alpha_1 = x_1 + y_1\sqrt{d}$,$\alpha_2 = x_2 + y_2\sqrt{d}$,$\alpha_3 = x_3 + y_3\sqrt{d}$ 给出方程 $x^2 - dy^2 = -1$ 的解,则

$$\alpha_1\alpha_2 = (x_1x_2 + dy_1y_2) + (x_1y_2 + x_2y_1)\sqrt{d}$$

而由引理 6.6.2,我们有

$$(x_1x_2 + dy_1y_2)^2 - d(x_1y_2 + x_2y_1)^2 = (x_1^2 - dy_1^2)(x_2^2 - dy_2^2) = 1$$

这就说明 $\alpha_1\alpha_2$ 给出方程 $x^2 - dy^2 = 1$ 的解。

$$\alpha_1\alpha_2\alpha_3 = x_1x_2x_3 + d(x_1y_2y_3 + x_2y_1y_3 + x_3y_1y_2) + (x_1x_2y_3 + x_2x_3y_1 + x_1x_3y_2 + dy_1y_2y_3)\sqrt{d}$$

而由引理 6.6.2,我们有

$$(x_1x_2x_3 + d(x_1y_2y_3 + x_2y_1y_3 + x_3y_1y_2))^2 - d(x_1x_2y_3 + x_2x_3y_1 + x_1x_3y_2 + dy_1y_2y_3)^2 = (x_1^2 - dy_1^2)(x_2^2 - dy_2^2)(x_3^2 - dy_3^2) = -1$$

这就说明 $\alpha_1\alpha_2\alpha_3$ 给出方程 $x^2 - dy^2 = -1$ 的解。

由引理 6.6.4 显然立刻就得出

引理 6.6.5

(1) 设 α 给出方程 $x^2 - dy^2 = 1$ 的解,则 $\alpha^n(n = 0, \pm 1, \pm 2, \cdots)$ 都给出它的解;

(2) 设 α 给出方程 $x^2 - dy^2 = -1$ 的解,则 $\alpha^{2n}(n = 0, \pm 1, \pm 2, \cdots)$ 都给出方程 $x^2 - dy^2 = 1$ 的解,$\alpha^{2n-1}(n = 0, \pm 1, \pm 2, \cdots)$ 都给出方程 $x^2 - dy^2 = -1$ 的解。

从引理 6.6.5 我们就可以看出,只要知道了方程 $x^2 - dy^2 = 1$ 或 $x^2 - dy^2 = -1$ 的一组特解,就可以求出这些方程组的无穷多组解来。但是与二元一次不定方程不一样,如果你这组特解取的不适当的话,虽然你可以求出无穷多组解来,却不一定能求出全部解来。例如,如果设 α 给出它们的一组特解,则根据引理 6.6.5 可知 α^2 或 α^3 就也给出它们的一组特解,但是假如你把这组特解代入到引理 6.6.5 中的公式中去,就会发现立刻少了许多解,比如公式 $\alpha^{2n}(n = 0, \pm 1, \pm 2, \cdots)$ 或 $\alpha^{3(2n-1)}(n = 0, \pm 1, \pm 2, \cdots)$ 就不能包括 α 这个解。

下面我们来说明,如果上述方程的特解取的适当的话,则引理 6.6.5 中所给出的公式就能够包括它们的所有解。

引理 6.6.6 设 $d > 0$ 是一个正整数,且不是完全平方数。x_1, x_2, y_1, y_2 都

是非负整数。$\alpha = x_1 + y_1\sqrt{d}$，$\beta = x_2 + y_2\sqrt{d}$ 给出方程 $x^2 - dy^2 = 1$ 或 $x^2 - dy^2 = -1$ 的解。则 $\alpha < \beta$ 的充分必要条件是 $x_1 < x_2$。

证明 设 $\alpha = x_1 + y_1\sqrt{d}$，$\beta = x_2 + y_2\sqrt{d}$，给出方程 $x^2 - dy^2 = 1$ 的解，$x_1 < x_2$。则因 x_1, x_2 都是非负整数，因此 $x_1^2 < x_2^2$。又因 $x_1^2 = dy_1^2 + 1$，$x_2^2 = dy_2^2 + 1$，故有 $dy_1^2 + 1 < dy_2^2 + 1$，$dy_1^2 < dy_2^2$。由于 y_1, y_2 非负，因此就得出 $y_1 < y_2$。再由 $x_1 < x_2$ 和 $y_1 < y_2$ 就得出 $\alpha = x_1 + y_1\sqrt{d} < \beta = x_2 + y_2\sqrt{d}$。

反之，设 $\alpha < \beta$，如果 $x_1 \geqslant x_2$，那么与上面类似，我们可以得出 $y_1 \geqslant y_2$，因此由 $x_1 \geqslant x_2$ 和 $y_1 \geqslant y_2$ 就得出 $\alpha \geqslant \beta$。这就导出矛盾，因此必须有 $x_1 < x_2$。

对 $\alpha = x_1 + y_1\sqrt{d}$，$\beta = x_2 + y_2\sqrt{d}$，给出方程 $x^2 - dy^2 = -1$ 的解的情况类似可证。

引理 6.6.7 设方程 $x^2 - dy^2 = 1$ 或方程 $x^2 - dy^2 = -1$ 存在非平凡解，则在给出它们的解集合中分别存在一个最小解。

证明 根据自然数的最小数原理，在所有给出方程 $x^2 - dy^2 = 1$ 的非平凡解 $\alpha = x + y\sqrt{d}$ 所组成的集合中必存在着一个使得 x 最小的解 $\alpha_0 = x_0 + y_0\sqrt{d}$，由引理 6.6.6 可知，这个解就是所有给出方程 $x^2 - dy^2 = 1$ 的非平凡解 $\alpha = x + y\sqrt{d}$ 所组成的集合中的最小解。

在方程 $x^2 - dy^2 = -1$ 存在非平凡解的情况下类似可证所有给出方程 $x^2 - dy^2 = -1$ 的非平凡解 $\alpha = x + y\sqrt{d}$ 所组成的集合中存在一个最小解。

定义 6.6.2 所有给出方程 $x^2 - dy^2 = 1$ 或方程 $x^2 - dy^2 = -1$ 的非平凡解 $\alpha = x + y\sqrt{d}$ 所组成的集合中的最小解分别称为方程 $x^2 - dy^2 = 1$ 或 $x^2 - dy^2 = -1$ 方程的生成元。

那么生成元有些什么性质呢？方程 $x^2 - dy^2 = -1$ 的生成元和方程 $x^2 - dy^2 = 1$ 的生成元之间又有什么关系呢？我们现在就来回答这些问题。

引理 6.6.8

(1) 设 θ 是方程 $x^2 - dy^2 = 1$ 或方程 $x^2 - dy^2 = -1$ 的生成元，则 $\theta > 1$；

(2) 设 α 是方程 $x^2 - dy^2 = -1$ 的生成元，β 是方程 $x^2 - dy^2 = 1$ 的生成元，则 $\alpha < \beta$；

(3) 如果 α 是方程 $x^2 - dy^2 = -1$ 的生成元，则 α^2 是方程 $x^2 - dy^2 = 1$ 的生成元；

(4) 设 $\alpha = x_2 + y_2\sqrt{d}$ 是方程 $x^2 - dy^2 = 1$ 的生成元，如果存在 $\theta = x_1 + y_1\sqrt{d}$，$x_1 > 0$，$y_1 > 0$，$x_1, y_1$ 都是整数，使得 $\theta^2 = \alpha$，则 θ 就是方程 $x^2 - dy^2 = -1$ 的生成元。

证明 (1) 设 $\theta = x_0 + y_0\sqrt{d}$，则根据生成元的定义可知 θ 首先是正的非平凡解，因此

$$\theta = x_0 + y_0\sqrt{d} > x_0 \geqslant 1$$

(2) 由引理 6.6.5 可知 α^2 给出方程 $x^2 - dy^2 = 1$ 的解，因此由 β 是方程 $x^2 - dy^2 = 1$ 的生成元或最小的非平凡解的定义可知 $\beta \leqslant \alpha^2$。如果 $\alpha \geqslant \beta$，那么由(1) 已证的性质 $\beta > 1$ 就得出 $\alpha^2 \geqslant \beta^2 \geqslant \beta$，这与 $\beta \leqslant \alpha^2$ 矛盾，因此必须有 $\alpha < \beta$。

(3) 由(2) 已证，α^2 给出方程 $x^2 - dy^2 = 1$ 的解，并且 $\beta \leqslant \alpha^2$，$\alpha < \beta$，所以必有 $\beta \leqslant \alpha^2 < \beta^2$，因而 $1 \leqslant \alpha^2\beta^{-1} < \beta$，由于 $\alpha^2\beta^{-1}$ 给出方程 $x^2 - dy^2 = 1$ 的解，而 β 是方程 $x^2 - dy^2 = 1$ 的最小解，因此必须有 $\alpha^2\beta^{-1} = 1$，这就说明必有 $\beta = \alpha^2$。

(4) 由 $\theta^2 = \alpha$ 推出 $x_1^2 + dy_1^2 = x_2, 2x_1y_1 = y_2$，因此

$$(x_1^2 - dy_1^2)^2 = x_2^2 - dy_2^2 = 1$$

故
$$x_1^2 - dy_1^2 = \pm 1$$

但是由于 α 给出方程 $x^2 - dy^2 = 1$ 的非平凡解中的最小者，而显然有 $0 < x_1 < x_2, 0 < y_1 < y_2$，所以有 $1 < \theta < \alpha$，因此 $x_1^2 - dy_1^2 \neq 1$(否则 θ 将给出方程 $x^2 - dy^2 = 1$ 的非平凡解，而这与 α 的最小性相矛盾)。这就证明了必须有 $x_1^2 - dy_1^2 = -1$，因此 θ 给出方程 $x^2 - dy^2 = -1$ 的非平凡解。再由 α 的最小性就得出 θ 的最小性，因而 θ 是方程 $x^2 - dy^2 = -1$ 的生成元。

定理 6.6.1

(1) 设方程 $x^2 - dy^2 = 1$ 存在生成元 θ，则 $\theta^n (n = 1,2,3,\cdots)$ 给出它的所有非平凡解；

(2) 设方程 $x^2 - dy^2 = -1$ 存在生成元 θ，则 $\theta^{2n-1} (n = 1,2,3,\cdots)$ 给出它的所有非平凡解。

证明 (1) 设(x^*, y^*)是方程 $x^2 - dy^2 = 1$ 的任一组非平凡解，则 $x^* > 0, y^* > 0$。令 $\alpha = x^* + y^*\sqrt{d}$，那么由于 θ 是生成元，因而 $\alpha \geqslant 0$。故存在整数 k 使得 $\theta^k \leqslant \alpha < \theta^{k+1}$，于是 $1 \leqslant \alpha\theta^{-k} < \theta$，然而由引理 6.6.3 和引理 6.6.4 可知 $\alpha\theta^{-k}$ 也给出方程 $x^2 - dy^2 = 1$ 的解，但根据 θ 的定义，θ 是给出方程 $x^2 - dy^2 = 1$ 的解并大于 1 中的最小者，而现在 $\alpha\theta^{-k}$ 却是一个给出方程 $x^2 - dy^2 = 1$ 的解并大于或等于 1 然而要比 θ 还要小的解，这就说明 $\alpha\theta^{-k}$ 只能等于 1。而由 $\alpha\theta^{-k} = 1$ 显然立即就得出 $\alpha = \theta^k$，这就证明了 $x^2 - dy^2 = 1$ 的任一组平凡解都可表示成 θ^k 的形式。

(2) (1) 设(x^*, y^*)是方程 $x^2 - dy^2 = -1$ 的任一组非平凡解，则 $x^* > 0, y^* > 0$。令 $\alpha = x^* + y^*\sqrt{d}$。那么由于 θ 是生成元，因而 $\alpha \geqslant \theta$。故存在整数 k 使得 $\theta^{2k-1} \leqslant \alpha < \theta^{2k+1}$，于是 $1 \leqslant \alpha\theta^{-(2k-1)} < \theta^2$，然而由引理6.6.3 和引理6.6.4 可知 $\alpha\theta^{-(2k-1)}$ 和 θ^2 也给出方程 $x^2 - dy^2 = 1$ 的解，由引理 6.6.8 可知 θ^2 是方

程 $x^2-dy^2=1$ 的最小解。而现在 $\alpha\theta^{-(2k-1)}$ 却是一个给出方程 $x^2-dy^2=1$ 的解并大于等于1然而要比 θ^2 还要小的解，这就说明 $\alpha\theta^{-(2k-1)}$ 只能等于1。而由 $\alpha\theta^{-(2k-1)}=1$ 显然立即就得出 $\alpha=\theta^{2k-1}$，这就证明了 $x^2-dy^2=-1$ 的任一组非平凡解都可表示成 θ^{2k-1} 的形式。

因此现在的全部问题就归结为确定方程 $x^2-dy^2=1$ 和方程 $x^2-dy^2=-1$ 存在生成元的条件以及在生成元存在的情况下如何求出生成元的问题了。下面我们就来研究这个问题。

引理6.6.9 设 $\alpha=[a_0;a_1,a_2,\cdots]$ 是一个实二次无理数，$r_n=[a_n;a_{n+1},a_{n+2},\cdots]$ 是 α 的余式，则对任意 n，r_n 可表为 $\dfrac{P_n+\sqrt{D}}{Q_n}$ 的形式，其中 P_n,Q_n 是整数，$D>0$ 是一个与 n 无关的正整数，且不是完全平方数，而 $Q_n\mid D-P_n^2$。

证明 由于 α 是一个实二次无理数，故 α 必满足一个既约的整系数二次方程

$$ax^2+bx+c=0,a>0,(a,b,c)=1$$

且 $\Delta=b^2-4ac>0$ 是一个非完全平方数，故

$$\alpha=\frac{-b+\sqrt{\Delta}}{2}\text{或}\alpha=\frac{-b-\sqrt{\Delta}}{2}$$

当 $\alpha=\dfrac{-b+\sqrt{\Delta}}{2}$ 时

$$\alpha=\frac{-2ab+\sqrt{4a^2\Delta}}{4a^2}=\frac{P_0+\sqrt{D}}{Q_0}$$

则 P_0,Q_0 是整数，$D>0$ 是一个正整数，且 $D-P_0^2=4a^2\Delta-4a^2b^2=-4acQ_0$，因此 $Q_0\mid D-P_0^2$。

当 $\alpha=\dfrac{-b-\sqrt{\Delta}}{2}$ 时

$$\alpha=\frac{2ab+\sqrt{4a^2\Delta}}{-4a^2}=\frac{P_0+\sqrt{D}}{Q_0}$$

则 P_0,Q_0 仍是整数，$D>0$ 是一个正整数，且 $D-P_0^2=4a^2\Delta-4a^2b^2=4acQ_0$，因此 $Q_0\mid D-P_0^2$。

因此引理对 $n=0$ 的情况成立

$$\frac{1}{r_1}=\alpha-a_0=\frac{P_0+\sqrt{D}}{Q_0}-a_0=\frac{\sqrt{D}-(a_0Q_0-P_0)}{Q_0}=$$

$$\frac{D-(a_0Q_0-P_0)^2}{Q_0(\sqrt{D}+a_0Q_0-P_0)}$$

令

$$P_1=a_0Q_0-P_0,Q_1=\frac{D-P_1^2}{Q_0}$$

那么$\frac{1}{r_1}=\frac{Q_1}{\sqrt{D}+P_1}$，因此 $r_1=\frac{P_1+\sqrt{D}}{Q_1}$，其中 P_1,Q_1 都是整数，且由 $Q_0\mid D-P_0^2$ 得出

$$D-P_0^2\equiv 0(\bmod Q_0),D-P_1^2\equiv D-P_0^2\equiv 0(\bmod Q_0)$$

因此 $Q_0\mid D-P_1^2$，但是 $D-P_1^2=Q_0Q_1$，故 $Q_1\mid D-P_1^2$。

因此引理对 $n=1$ 的情况也成立。

依次类推就得出如果 $r_n=\frac{P_n+\sqrt{D}}{Q_n}$，其中 P_n,Q_n 都是整数，且 $Q_n\mid D-P_n^2$，则由 $a_n=[r_n]$，$r_n=a_n+\frac{1}{r_{n+1}}$，并令 $P_{n+1}=a_nQ_n-P_n$，$Q_{n+1}=\frac{D-P_n^2}{Q_n}$ 可得出 $r_{n+1}=\frac{P_{n+1}+\sqrt{D}}{Q_{n+1}}$，$Q_{n+1}\mid D-P_{n+1}^2$。这就证明了引理。

从引理证明的过程中就看出 D 与 n 无关，而且由于 $D>0$ 不是完全平方数，所以 $Q_0,Q_1,Q_2,\cdots$ 都不为 0，因此 Q_n 的定义式都是有意义的。

引理 6.6.10 设 $\alpha=[a_0;a_1,a_2,\cdots]$ 是一个实二次无理数，$r_n=[a_n;a_{n+1},a_{n+2},\cdots]$ 是 α 的余式，$r_n=\frac{P_n+\sqrt{D}}{Q_n}$，其中 P_n,Q_n 是整数，$D>0$ 是一个与 n 无关的正整数，且不是完全平方数，而 $Q_n\mid D-P_n^2$（引理6.6.9保证了 r_n 一定可表为所说的形式）。$\frac{p_n}{q_n}$ 是 α 的第 n 阶渐近分数，则

(1) $(p_{n-1}p_{n-2}Q_0-(p_{n-1}q_{n-2}+p_{n-2}q_{n-1})P_0)-q_{n-1}q_{n-2}\frac{D-P_0^2}{Q_0}=(-1)^{n+1}P_n$；

(2) $(p_{n-1}Q_0-q_{n-1}P_0)^2-q_{n-1}^2D=(-1)^nQ_0Q_n$。

证明 由定理 6.1.1 可知

$$\alpha=\frac{p_{n-1}r_n+p_{n-2}}{q_{n-1}r_n+q_{n-2}}$$

又由引理 6.6.8 的证明过程可知

$$\alpha=\frac{P_0+\sqrt{D}}{Q_0},r_n=\frac{P_n+\sqrt{D}}{Q_n}$$

把这两个式子代入到上式中就得到

$$\frac{P_0+\sqrt{D}}{Q_0}=\frac{p_{n-1}(P_n+\sqrt{D})+p_{n-2}Q_n}{q_{n-1}(P_n+\sqrt{D})+q_{n-2}Q_n}$$

把上式去分母相乘展开再比较有理部分和$\sqrt{D}$ 的系数最后可得

$$q_{n-1}P_n+q_{n-2}Q_n=p_{n-1}Q_0-q_{n-1}P_0$$

$$(p_{n-1}Q_0 - q_{n-1}P_0)P_n + (p_{n-2}Q_0 - q_{n-2}P_0)Q_n = q_{n-1}D$$

把 P_n, Q_n 看成未知数，把上面两式看成是关于它们的二元一次方程组，从上面两式中解出 P_n, Q_n 来，并利用 $q_np_{n-1} - p_nq_{n-1} = (-1)^n$ 及 $Q_0 \mid D - P_0^2$ 即可得到所要证明的式子。

引理 6.6.11 设 $\frac{p_n}{q_n}$ 是 $\sqrt{d}$ 的连分式的渐近分数，则存在两串数 $P_n, Q_n (n \geqslant 0)$ 使得

$$p_{n-1}p_{n-2} - dq_{n-1}q_{n-2} = (-1)^{n+1}P_n$$
$$p_{n-1}^2 - dq_{n-1}^2 = (-1)^nQ_n$$

证明 在引理 6.6.9 中取 $\alpha = \sqrt{d}$，则可取 $P_0 = 0, Q_0 = 1, D = d$，并且存在两串整数 $P_n, Q_n (n \geqslant 0)$ 使得 $Q_n \mid d - p_n^2$，再由引理 6.6.10 即得 P_n, Q_n 满足关系式

$$p_{n-1}p_{n-2} - dq_{n-1}q_{n-2} = (-1)^{n+1}P_n$$

和

$$p_{n-1}^2 - dq_{n-1}^2 = (-1)^nQ_n$$

引理 6.6.12

(1) 设 $d > 0$ 是一个正整数，且不是完全平方数，那么 $\alpha = \sqrt{d} + [\sqrt{d}]$ 是一个纯循环连分数；

(2) 设 l 是 α 的连分数表示式中循环节的长度，P_n, Q_n 是引理 6.6.9 中由 α 所确定的整数，则 $Q_k = 1$ 的充分必要条件是 $l \mid k$；

(3) 对任意的 $n \geqslant 0$，Q_n 不可能等于 -1。

证明 (1) 显然 $\alpha > 1$，又 $\alpha' = -\sqrt{d} + [\sqrt{d}] = -\{\sqrt{d}\}$，故 $-1 < \alpha' < 0$（由于 d 不是完全平方数，因此 $\{\sqrt{d}\} \neq 0$）。这说明 α 是既约的，因此根据定理 6.3.3 可知 α 必可表示成一个纯循环连分数。

(2) 在(1)中已证，α 必可表示成一个纯循环连分数。因此根据定理 6.3.4 可知对任意 $n > 0$，r_n 也是纯循环的，而由引理 6.6.9 又有

$$r_n = \frac{P_n + \sqrt{d}}{Q_n}$$

因此立刻就得出

$Q_k = 1 \Leftrightarrow r_k = \sqrt{d} + P_k$ 是纯循环连分数 $\Leftrightarrow$

$r_k = \sqrt{d} + P_k$ 是既约的实二次无理数（定理 6.3.2）$\Leftrightarrow$

$r_k = \sqrt{d} + P_k > 1,\ -1 < -\sqrt{d} + P_k = r'_k < 0 \Leftrightarrow$

$P_k < \sqrt{d} < P_k + 1 \Leftrightarrow [\sqrt{d}] = P_k \Leftrightarrow$

$r_k = \sqrt{d} + P_k = \sqrt{d} + [\sqrt{d}] = \alpha \Leftrightarrow$

$l \mid k$（定理 6.3.4）

(3) 由(2)中的证明可知

$$Q_n = -1 \Leftrightarrow r_n = -\sqrt{d} - P_n \text{ 是纯循环连分数} \Rightarrow$$
$$r_n = -\sqrt{d} - P_n \text{ 是既约的实二次无理数(定理 6.3.2)} \Leftrightarrow$$
$$r_n = -\sqrt{d} - P_n > 1, -1 < \sqrt{d} - P_n = r'_n < 0 \Leftrightarrow$$
$$-\sqrt{d} - 1 > P_n > \sqrt{d}$$

而这显然是不可能的,故对任意 $n \geqslant 0$, Q_n 不可能等于 -1。

引理 6.6.13 设 $d > 0$ 是正整数,且不是完全平方数。$x_0 > 0$, $y_0 > 0$ 是不定方程 $x^2 - dy^2 = 1$ 或者不定方程 $x^2 - dy^2 = -1$ 的解,则 $\frac{x_0}{y_0}$ 必为 $\sqrt{d}$ 的某个渐近分数 $\frac{p_n}{q_n}$,且 $x_0 = p_n$, $y_0 = q_n$。

证明 (1) 由 $x_0^2 - dy_0^2 = \pm 1$ 和定理 3.3.7 可知 $(x_0, y_0) = 1$;

(2) 如果 $x_0 < y_0$,则 $\pm 1 = x_0^2 - dy_0^2 < y_0^2 - dy_0^2 \leqslant -y_0^2 \leqslant -1$,得出矛盾,因此必有

$$x_0 \geqslant y_0$$

(3)
$$\left|\sqrt{d} - \frac{x_0}{y_0}\right| = \frac{\left|d - \frac{x_0^2}{y_0^2}\right|}{\sqrt{d} + \frac{x_0}{y_0}} = \frac{|x_0^2 - dy_0^2|}{y_0^2\left(\sqrt{d} + \frac{x_0}{y_0}\right)} = \frac{1}{y_0^2\sqrt{d} + x_0 y_0} < \frac{1}{y_0^2 + y_0^2} < \frac{1}{2y_0^2}$$

故由定理 6.2.4 知 $\frac{x_0}{y_0}$ 必为 $\sqrt{d}$ 的某个渐近分数 $\frac{p_n}{q_n}$。又(1)已证明 $\frac{x_0}{y_0}$ 和 $\frac{p_n}{q_n}$ 都是既约分数,故由 $\frac{x_0}{y_0} = \frac{p_n}{q_n}$ 就得出 $x_0 = p_n$, $y_0 = q_n$。

定理 6.6.2 设 $\sqrt{d}$ 的循环连分数的周期为 l,渐近分数为 $\frac{p_n}{q_n}$,那么

(1) 当 l 为偶数时,不定方程 $x^2 - dy^2 = -1$ 无解,而不定方程 $x^2 - dy^2 = 1$ 的生成元为 $\theta = p_{l-1} + q_{l-1}\sqrt{d}$;

(2) 当 l 为奇数时,不定方程 $x^2 - dy^2 = -1$ 的生成元 $\theta = p_{l-1} + q_{l-1}\sqrt{d}$,因而不定方程 $x^2 - dy^2 = 1$ 的生成元为 $\theta^2 = p_{2l-1} + q_{2l-1}\sqrt{d}$。

证明 由引理 6.6.13 知如果 $x_0 + y_0\sqrt{d}$ 给出不定方程 $x^2 - dy^2 = 1$ 或者不定方程 $x^2 - dy^2 = -1$ 的非平凡解,则必存在 $\sqrt{d}$ 的连分式表示的某个渐近分数 $\frac{p_n}{q_n}$,使得

$$x_0 = p_n, y_0 = q_n$$

又由引理6.6.11知

$$p_n^2 - dq_n^2 = (-1)^{n+1}Q_{n+1}$$

其中 P_n, Q_n 是引理6.6.9中由 $\sqrt{d}$ 所确定的整数。又显然 $\sqrt{d}$ 和 $\sqrt{d}+[\sqrt{d}]$ 的连分式表示中的余式在 $n\geqslant 1$ 时相同，因而由引理6.6.9中确定 P_n 和 Q_n 的方法知，当 $n\geqslant 1$ 时 $\sqrt{d}$ 和 $\sqrt{d}+[\sqrt{d}]$ 确定了相同的 P_n 和 Q_n。又由直接计算可知

$$P_0(\sqrt{d}) = 0, Q_0(\sqrt{d}) = 1, P_0(\sqrt{d}+[\sqrt{d}]) = [\sqrt{d}], Q_0(\sqrt{d}+[\sqrt{d}]) = 1$$

因此对 $n\geqslant 0$，$\sqrt{d}$ 和 $\sqrt{d}+[\sqrt{d}]$ 确定了完全相同的 Q_n。

由引理6.6.12知对任意 $n\geqslant 0$，$Q_n\neq -1$，$Q_n = 1 \Leftrightarrow l\mid n$，其中 l 是 $\sqrt{d}$ 的循环连分式表示的周期，同时也是 $\sqrt{d}+[\sqrt{d}]$ 的循环连分式表示的周期。因此由

$$p_n^2 - dq_n^2 = (-1)^{n+1}Q_{n+1}$$

可知 p_n, q_n 是不定方程 $x^2-dy^2=1$ 或者不定方程 $x^2-dy^2=-1$ 的非平凡解 $\Leftrightarrow Q_{n+1}=1 \Leftrightarrow l\mid(n+1) \Leftrightarrow n+1=kl$，这时

$$p_{kl-1}^2 - dq_{kl-1}^2 = (-1)^{kl}$$

由此就得出当 l 是偶数时，不定方程 $x^2-dy^2=-1$ 无解，而不定方程 $x^2-dy^2=1$ 的生成元为 $\theta = p_{l-1}+q_{l-1}\sqrt{d}$。

当 l 是奇数时，不定方程 $x^2-dy^2=-1$ 的生成元为 $\theta = p_{l-1}+q_{l-1}\sqrt{d}$，从而根据引理6.6.8，不定方程 $x^2-dy^2=1$ 的生成元为 $\theta^2 = p_{2l-1}+q_{2l-1}\sqrt{d}$。

至此，我们已完全解决了两类 Pell 方程有解的条件和在有解时如何求出解的表达公式的问题。在当初刚一接触到这一问题时，你恐怕很难想到它们是不是有解竟要由 $\sqrt{d}$ 的循环连分式表示的周期的奇偶性来决定，甚至恐怕连 $\sqrt{d}$ 的连分式表示式一定是循环的也不一定能想象得到吧！而这样一个难以想象的答案一旦水落石出，完全得出后，也一定心情十分愉快吧！这就是科学研究的乐趣，科学研究的乐趣就在于不管经过多少艰难曲折而百折不挠的最后弄清事物的真相后研究者内心所得到的满足，就在于在没有得出答案之前决心要一直探索下去的内心的强烈的欲望。

习题6.6

1. 求出下列 Pell 方程的生成元

(1) $x^2-7y^2=-1$　　(2) $x^2-7y^2=1$

(3) $x^2-13y^2=-1$　　(4) $x^2-7y^2=1$

(5) $x^2-74y^2=-1$　　(6) $x^2-74y^2=1$

(7) $x^2-87y^2=-1$　　(8) $x^2-87y^2=-1$

2. 解下列 Pell 方程

(1) $x^2-80y^2=-1$　　(2) $x^2-80y^2=1$

(3) $x^2-23y^2=-1$　　(4) $x^2-23y^2=1$

(5) $x^2-28y^2=-1$　　(6) $x^2-28y^2=1$

(7) $x^2-29y^2=-1$　　(8) $x^2-29y^2=1$

(9) $x^2-61y^2=-1$　　(10) $x^2-61y^2=1$

3. 设 $d>0$ 是正整数，且是非平方数，a 是给定的正整数。证明：$x^2-dy^2=1$ 有无穷多组解满足 $a\mid y$。

4. 求不定方程 $x^2+(x+1)^2=y^2$ 的所有正整数解，并说明它们的几何意义。

5. 求出 $x^2+2xy-2y^2=1$ 的三组非平凡解。

6. (1) 证明：如果 $a^2>b$，且 a^2-b 不是完全平方数，则 $x^2+2axy+by^2=1$ 有无穷多组解；

(2) 如果 $a^2<b$，则(1) 中方程的所有解中，必有 $y=-1,0$ 或 1；

(3) 如果 $a^2=b$，会发生什么情况？

7. (1) 设 $a=2mn,b=m^2-n^2,c=m^2+n^2$ 是一个直角三角形的三条边，如果 $b=a+1$，证明：$(m-n)^2-2n^2=1$，并求出所有这种三角形；

(2) 求出上述三角形中最小的两个。

8. (1) 证明：当且仅当 $3(a^2-1)$ 是完全平方数时，以 $2a-1,2a,2a+1$ 为边长的三角形的面积是整数；

(2) 试找出三个这样的三角形；

(3) 证明：当且仅当 $3((2a+1)^2-4)$ 是完全平方数时，以 $2a,2a+1,2a+2$ 为边长的三角形的面积是有理数；

(4) 证明：不可能存在上述情况。

9. 设 $x_n+y_n\sqrt{2}=(1+\sqrt{2})^n$，证明：

(1) $x_{n+1}=y_{n+1}+y_n,y_{n+1}=x_n+y_n,n\geqslant 1$；

(2) $y_{2n+1}=y_{n+1}^2+y_n^2,n\geqslant 1$；

(3) y_{n+1}^2 是两个相邻自然数的平方和，求出这两个自然数；

(4) 设 $x_0=1,y_0=0$，证明：当 $n\geqslant m$ 时

$$x_nx_m-2y_ny_m=(-1)^m x_{n-m}$$

$$x_ny_m-y_nx_m=(-1)^m y_{n-m}$$

(5) $x_{2n+1}=x_{n+1}x_n+2y_{n+1}y_n=2x_{n+1}x_n+(-1)^{n+1}$；

$y_{2n+1}=x_{n+1}y_n+y_{n+1}x_n$；

(6) $2\mid y_{2n},2\nmid y_{2n+1}$；

(7) 当 $n>1$ 时，x_n 不是完全平方数。

10. (1) 证明：当 $d\equiv 3\pmod 4$ 时，不定方程 $x^2-dy^2=-1$ 无解；

(2) 设 $p\equiv 1(\mathrm{mod}\ 4)$ 是一个素数,证明:不定方程 $x^2-dy^2=-1$ 必有解。

11. 设 $d>0$ 是正整数,且是非平方数,k 是整数。证明:如果 $x^2-dy^2=k$ 有一组解,它就有无限多组解。

12. 设 $d>0$ 是正整数,且是非平方数,k 是整数,$|c|<\sqrt{d}$。如果正整数 x_0,y_0 是 $x^2-dy^2=k$ 的一组解,且 $(x_0,y_0)=1$,则 $\frac{x_0}{y_0}$ 必为 $\sqrt{d}$ 的渐近分数。

13. 能否对不定方程 $x^2-dy^2=\pm 4$ 给出一个类似于对于不定方程 $x^2-dy^2=\pm 1$ 那样的完整讨论来(什么时候有解)以及在有解时,解的结构和公式是怎样的?

14. 设 $d>0$ 是正整数,且是非平方数。正整数 x_0,y_0 是不定方程 $x^2-dy^2=1$ 的一组解。证明:如果 $x_0>\frac{y_0^2}{2}-1$,则 $\theta=x_0+y_0\sqrt{d}$ 是不定方程 $x^2-dy^2=1$ 的生成元。

6.7 连分数的应用 Ⅳ:把整数表为平方和

在第三章例 3.6.7 中我们已经用同余类的方法证明了方程 $x^2+y^2=1\ 955$ 不存在整数解。这个问题反过来说就是 1 995 这个数不可能表示成两个整数的平方和。于是很自然的,由此问题出发我们可以提出一个一般的问题,那就是

自然数 n 在满足什么条件时,才能表示成为两个整数的平方和?如果能表示,那么如何表示?又在什么条件下,这种表示方法是唯一的?更一般的,我们还可以问,在 n 满足什么条件时,不定方程 $x^2+ay^2=n$ 有解?等等。这一节我们就来研究这些问题。

引理 6.7.1 设 $(x,ay)=1$,p 是二次型 x^2+ay^2 的大于 2 的素因数,则 $\left(\frac{-a}{p}\right)=1$。

证明 设 $p>2$ 是任意奇素数,$p\mid x^2+ay^2$,则 $x^2+ay^2\equiv 0(\mathrm{mod}\ p)$,因此 $x^2\equiv -ay^2(\mathrm{mod}\ p)$。这说明 $-ay^2$ 是数 p 的平方剩余(复习第三章 3.10 二次同余式),因此

$$\left(\frac{-ay^2}{p}\right)=\left(\frac{-a}{p}\right)\left(\frac{y^2}{p}\right)=\left(\frac{-a}{p}\right)=1$$

这就证明了引理。

引理 6.7.2 设 $(u,v)=1$,则二次型 x^2-a 和二次型 v^2-au^2 的素因数相同。

证明 (1) 令 $u=1$,则 $v^2-au^2=v^2-a$,因此就得出二次型 x^2-a 只不

过是二次型 v^2-au^2 的一种特殊情况，因而自然被包括在后者中，这就说明二次型 x^2-a 的素因数都是二次型 v^2-au^2 的素因数。

(2) 设 p 是二次型 v^2-au^2 的素因数，则 $v^2-au^2\equiv 0(\bmod p)$，则必有 $p\nmid u$，否则由 $p\mid u$ 得出 $p\mid v$，而这与 $(u,v)=1$ 的假设矛盾。也就是说，必有 $(u,p)=1$，因此由一次同余式方程的理论知（见第三章定理 3.9.3）一次同余式方程 $ux\equiv 1(\bmod p)$ 必有解，或者必存在 ξ 使得 $u\xi\equiv 1(\bmod p)$。因此由 $v^2-au^2\equiv 0(\bmod p)$ 和 $u\xi\equiv 1(\bmod p)$ 就得到

$$\xi^2v^2-au^2\xi^2\equiv 0(\bmod p)$$

$$(\xi v)^2-a\equiv 0(\bmod p)$$

这就说明，p 是二次型 x^2-a 的素因子。

由引理 6.7.2 我们又重新得到引理 6.7.1。

当方程 $x^2+ay^2=n$ 有解 (x_0,y_0) 时，显然 $(x_0,-y_0)$，$(-x_0,y_0)$，$(-x_0,-y_0)$ 也是解，当 $a=1$ 时，(y_0,x_0) 以及加上符号搭配而得的有序对也都是解。我们认为这些解在本质上是相同的。因此以下只须考虑方程 $x^2+ay^2=n$ 的正解即可。

引理 6.7.3 设 $0<a<p$，其中 p 是一个奇素数，则方程 $x^2+ay^2=p$ 的解必是互素的，且在有解时，本质上不同的解是唯一的。

证明 方程 $x^2+ay^2=p$ 的解（如果有）(x_0,y_0) 显然必须是互素的，否则方程式的左边将大于 p，因而方程 $x^2+ay^2=p$ 将不可能有解。

现设 (x_1,y_1)，(x_2,y_2) 是方程 $x^2+ay^2=p$ 的两个不同的解。

用 y_2^2 乘以等式 $x_1^2+ay_1^2=p$ 的两边，用 y_1^2 乘以等式 $x_2^2+ay_2^2=p$ 的两边，并将所得的两个式子相减就得到

$$(x_1y_2-x_2y_1)(x_1y_2+x_2y_1)=p(y_2^2-y_1^2)$$

因此必有 $p\mid x_1y_2-x_2y_1$ 或者 $p\mid x_1y_2+x_2y_1$。又

$$(x_1y_2-x_2y_1)+(x_1y_2+x_2y_1)=2x_1y_2$$

如果 $p\mid 2x_1y_2$，那么 $p\mid x_1y_2$，因而 $p\mid x_1$ 或者 $p\mid y_2$。无论发生哪一种情况，由此都将得出方程式 $x^2+ay^2=p$ 的左边将大于 p，因而方程 $x^2+ay^2=p$ 将不可能有解，故 $p\nmid x_1y_2$。由于

$$(x_1y_2-x_2y_1)+(x_1y_2+x_2y_1)=2x_1y_2$$

这就说明不可能同时成立关系式 $p\mid x_1y_2-x_2y_1$ 和 $p\mid x_1y_2+x_2y_1$。也就是说只可能发生两种情况：或者 $p\mid x_1y_2-x_2y_1$，或者 $p\mid x_1y_2+x_2y_1$，而且这两种情况之一必然会发生。

将等式 $x_1^2+ay_1^2=p$ 和等式 $x_2^2+ay_2^2=p$ 的两边相乘就得到

$$(x_1x_2+ay_1y_2)^2+a(x_1y_2-x_2y_1)^2=(x_1^2+ay_1^2)(x_2^2+ay_2^2)=p^2$$

以及 $(x_1x_2-ay_1y_2)^2+a(x_1y_2+x_2y_1)^2=(x_1^2+ay_1^2)(x_2^2+ay_2^2)=p^2$

以下分两种不同的情况来讨论。

(1) $a>1$。如果 $p\mid x_1y_2+x_2y_1$,则由于 $x_1y_2+x_2y_1>0$,因此

$$x_1y_2+x_2y_1=np,n\geqslant 1$$

但由于$(x_1x_2+ay_1y_2)^2+a(x_1y_2-x_2y_1)^2=p^2$及 $a>1$,故这是不可能的。因此只可能 $p\mid x_1y_2-x_2y_1$,这时由等式$(x_1x_2+ay_1y_2)^2+a(x_1y_2-x_2y_1)^2=p^2$及 $a>1$ 得出

$$x_1y_2-x_2y_1=0\text{ 或}\frac{x_1}{y_1}=\frac{x_2}{y_2}$$

而由于$(x_1,y_1)=1,(x_2,y_2)=1$,因此必有 $x_1=x_2,y_1=y_2$。

(2) $a=1$。如果 $p\mid x_1y_2+x_2y_1$,那么 $x_1y_2+x_2y_1=p$。因此由等式$(x_1x_2-ay_1y_2)^2+a(x_1y_2+x_2y_1)^2=p^2$ 得出

$$x_1x_2-y_1y_2=0\text{ 或}\frac{x_1}{y_1}=\frac{y_2}{x_2}$$

而由于$(x_1,y_1)=1,(x_2,y_2)=1$,因此必有 $x_1=y_2,y_1=x_2$。因此我们得到本质上相同的解。

如果 $p\mid x_1y_2-x_2y_1$,那么与(1)中的证明类似可以得出

$$x_1y_2-x_2y_1=0\text{ 或}\frac{x_1}{y_1}=\frac{x_2}{y_2}$$

而由于$(x_1,y_1)=1,(x_2,y_2)=1$,因此必有 $x_1=x_2,y_1=y_2$。

引理 6.7.4 设 t 是同余式$x^2\equiv-a\pmod p$的解,且$0<t<\frac{p}{2}$,$\frac{p_k}{q_k}$是$\frac{t}{p}$的满足条件 $q_k<\sqrt{p}<q_{k+1}$ 的渐近分数,则

(1) $(tq_k-pp_k)^2+aq_k^2<(a+1)p$ 且 $p\mid(tq_k-pp_k)^2+aq_k^2$;

(2) 用 $p-t$ 代替(1)中的 t,则(1)中的结论仍然成立。

证明 (1) 设$\frac{t}{p}=[0;a_1,a_2,\cdots,a_m]$,则

$$\frac{p_0}{q_0}=\frac{0}{1},\frac{p_1}{q_1}=\frac{1}{a_1},\cdots,\frac{p_m}{q_m}=\frac{t}{p}$$

由于 $q_0=1<\sqrt{p}$,$q_m=p>\sqrt{p}$,因此必存在一个下标 k 使得$q_k<\sqrt{p}<q_{k+1}$。于是

$$\left|\frac{t}{p}-\frac{p_k}{q_k}\right|=\frac{|tq_k-pp_k|}{pq_k}<\frac{1}{q_kq_{k+1}}\text{(定理 6.2.2)}$$

由此得出

$$(tq_k-pp_k)^2<\frac{p^2}{q_{k+1}^2}<\frac{p^2}{p}=p$$

$$(tq_k - pp_k)^2 + aq_k^2 < p + ap = (a+1)p$$

又 $$(tq_k - pp_k)^2 + aq_k^2 = (t^2 + a)q_k^2 + (2tp_kq_k + pp_k^2)p \equiv 0 \pmod p$$

故 $$p \mid (tq_k - pp_k)^2 + aq_k^2$$

(2) 同余式 $x^2 \equiv -a \pmod p$ 的另一个解即是 $p-t$，$p - t > \frac{p}{2}$，则

$$\frac{t}{p} = \frac{1}{z}, z = [a_1; a_2, \cdots, a_m], \frac{p-t}{p} = 1 - \frac{1}{z} = \frac{z-1}{z}$$

故 $\frac{p-t}{p} = [0; \frac{z}{z-1}] = [0; 1, \frac{1}{z-1}] = [0; 1, z-1] = [0; 1, a_1 - 1, a_2, \cdots, a_m]$

由于 $t < \frac{p}{2}$，所以 $\frac{t}{p} < \frac{1}{2}$，故 $a_1 - 1 > 0$，这说明 $[0; 1, a_1 - 1, a_2, \cdots, a_m]$ 是一个简单连分数。由此看出当 $k \geqslant 2$ 时，$\frac{t}{p}$ 和 $\frac{p-t}{p}$ 的连分式表示的元素完全一样。设 $\frac{p'_i}{q'_i}$ 表示 $\frac{p-t}{p}$ 的渐近分数，则通过直接计算容易验证

$$q'_{i+1} = q_i, p'_{i+1} = q_i - p_i, i > 1$$

因此 $$q'_{k+1} < \sqrt{p} < q'_{k+2}$$

$$(p-t)q'_{k+1} - pp'_{k+1} = -tq'_{k+1} + p(q'_{k+1} - p'_{k+1}) =$$
$$-tq_k + pp_k = -(tq_k - pp_k)$$

因此当我们用 $p-t$ 代替(1)中的 t 后，关系式

$$(tq_k - pp_k)^2 + aq_k^2 < (a+1)p$$

和关系式 $$p \mid (tq_k - pp_k)^2 + aq_k^2$$

仍然成立。

定理 6.7.1 设 p 是一个素数，则方程 $x^2 + y^2 = p$ 有整数解的充分必要条件是 $p = 2$ 或者 $p \equiv 1 \pmod 4$。且在有解时，本质上不同的解是唯一的。

证明 必要性：设方程 $x^2 + y^2 = p$ 有整数解，则由于 p 是素数，故必有 $(x, y) = 1$，因此由引理 6.7.1 知或者 $p = 2$，或者 $\left(\frac{-1}{p}\right) = 1$。因此由引理 3.10.3 就得出 $p = 2$ 或者 $p \equiv 1 \pmod 4$。

充分性：当 $p = 2$ 时，显然方程 $x^2 + y^2 = 2$ 有整数解 $x = y = 1$。现设 $p \equiv 1 \pmod 4$ 是奇素数。那么 $\left(\frac{-1}{p}\right) = 1$，因此同余式 $x^2 \equiv -1 \pmod p$ 有解。设 t 是同余式 $x^2 \equiv -1 \pmod p$ 的解，且 $0 < t < \frac{p}{2}$。$\frac{p_k}{q_k}$ 是 $\frac{t}{p}$ 的满足条件 $q_k < \sqrt{p} < q_{k+1}$ 的渐近分数，则由引理 6.7.4 知

$$(tq_k - pp_k)^2 + q_k^2 < 2p$$

由于 $$p \mid (tq_k - pp_k)^2 + q_k^2$$

故必有 $$(tq_k - pp_k)^2 + q_k^2 = p$$

这就证明了方程 $x^2+y^2=p$ 有整数解。

由引理 6.7.3 知有解时，当方程 $x^2+y^2=p$ 有整数解时，本质上不同的解是唯一的。

定理 6.7.2 设 p 是一个素数，则方程 $x^2+2y^2=p$ 有整数解的充分必要条件是 $p=2$ 或者 $p\equiv 1 \pmod 8$ 或者 $p\equiv 3 \pmod 8$。且在有解时，本质上不同的解是唯一的。

证明 必要性：设方程 $x^2+2y^2=p$ 有整数解，则由于 p 是素数，故必有 $(x,2y)=1$，因此由引理 6.7.1 知或者 $p=2$，或者 $\left(\frac{-2}{p}\right)=1$。由勒让德符号的计算法则得出

$$\left(\frac{-2}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)=1$$

因此 $\left(\frac{-1}{p}\right)$ 和 $\left(\frac{2}{p}\right)$ 同号，这也就是说，它们都等于 1 或 -1。

当 $\left(\frac{-1}{p}\right)=\left(\frac{2}{p}\right)=1$ 时，由引理 3.10.3 得出 $p\equiv 1 \pmod 4$，$p\equiv \pm 1 \pmod 8$，因此 $p\equiv 1 \pmod 8$。

当时 $\left(\frac{-1}{p}\right)=\left(\frac{2}{p}\right)=-1$，由引理 3.10.3 得出 $p\equiv 3 \pmod 4$，$p\equiv \pm 3 \pmod 8$，因此 $p\equiv 3 \pmod 8$。

因此最后我们得到 $p=2$ 或者 $p\equiv 1 \pmod 8$ 或者 $p\equiv 3 \pmod 8$。

充分性：当 $p=2$ 时，显然方程 $x^2+2y^2=2$ 有整数解 $x=0, y=1$。

当 $p\equiv 1 \pmod 8$ 或者 $p\equiv 3 \pmod 8$ 时，$\left(\frac{-2}{p}\right)=1$，因此同余式 $x^2\equiv -2 \pmod p$ 有解。设 t 是同余式 $x^2\equiv -2 \pmod p$ 的解，且 $0<t<\frac{p}{2}$。$\frac{p_k}{q_k}$ 是 $\frac{t}{p}$ 的满足条件 $q_k<\sqrt{p}<q_{k+1}$ 的渐近分数，则由引理 6.7.4 知

$$(tq_k-pp_k)^2+2q_k^2<3p$$

由于 $p \mid (tq_k-pp_k)^2+2q_k^2$，故 $(tq_k-pp_k)^2+2q_k^2=p$ 或 $2p$。

如果 $(tq_k-pp_k)^2+2q_k^2=p$，则显然方程 $x^2+2y^2=p$ 有整数解。

如果 $(tq_k-pp_k)^2+2q_k^2=2p$，则显然 tq_k-pp_k 必为偶数，因此可设 $tq_k-pp_k=2v$，由此得出 $4v^2+2q_k^2=2p$，$q_k^2+2v^2=p$，因此这时方程 $x^2+2y^2=p$ 仍有整数解。

由引理 6.7.3 知有解时，当方程 $x^2+2y^2=p$ 有整数解时，本质上不同的解是唯一的。

定理 6.7.3 设 p 是一个素数，则方程 $x^2+3y^2=p$ 有整数解的充分必要条件是 $p=3$ 或者 $p\equiv 1 \pmod 6$。且在有解时，本质上不同的解是唯一的。

证明　必要性：设方程 $x^2+3y^2=p$ 有整数解，则由于 p 是素数，故必有 $(x,3y)=1$，因此由引理6.7.1知或者 $p=3$，或者 $\left(\frac{-3}{p}\right)=1$。由引理3.10.3和二次互反律得出

$$\left(\frac{-3}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)=(-1)^{\frac{p-1}{2}}\left(\frac{3}{p}\right)=$$

$$(-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}}(-1)^{\frac{3-1}{2}}\left(\frac{p}{3}\right)=\left(\frac{p}{3}\right)$$

由引理3.10.3可知 $\left(\frac{p}{3}\right)=1$ 的充分必要条件是 $p\equiv1(\mathrm{mod}\ 3)$，又 $p\equiv1(\mathrm{mod}\ 2)$，故 $p\equiv1(\mathrm{mod}\ 6)$。

因此最后我们得到 $p=3$ 或者 $p\equiv1(\mathrm{mod}\ 6)$。

充分性：当 $p=3$ 时，显然方程 $x^2+3y^2=3$ 有整数解 $x=0,y=1$。现设 $p\equiv1(\mathrm{mod}\ 6)$，那么 $\left(\frac{-3}{p}\right)$，因此同余式 $x^2\equiv-3(\mathrm{mod}\ p)$ 有解。设 t 是同余式 $x^2\equiv-3(\mathrm{mod}\ p)$ 的解，且 $0<t<\frac{p}{2}$。$\frac{p_k}{q_k}$ 是 $\frac{t}{p}$ 的满足条件 $q_k<\sqrt{p}<q_{k+1}$ 的渐近分数，则由引理6.7.4知

$$(tq_k-pp_k)^2+3q_k^2<4p$$

由于 $p\mid(tq_k-pp_k)^2+3q_k^2$，故 $(tq_k-pp_k)^2+3q_k^2=p,2p$ 或 $3p$。为叙述简明，设 $\lambda=tq_k-pp_k$，于是 $\lambda^2+3q_k^2=p,2p$ 或 $3p$。

我们首先证明，不可能发生 $\lambda^2+3q_k^2=2p$ 的情况，假设不然有 $\lambda^2+3q_n^2=2p$，那么显然 λ 和 q_k 不可能一个是奇数，一个是偶数，也就是说，λ 和 q_k 必须同时是奇数或同时是偶数。如果 λ 和 q_k 都是偶数，则有 $\lambda^2+3q_k^2\equiv0(\mathrm{mod}\ 4)$，如果 λ 和 q_k 都是奇数，则 $\lambda^2\equiv1(\mathrm{mod}\ 4)$，$q_k^2\equiv1(\mathrm{mod}\ 4)$，这时仍得出 $\lambda^2+3q_k^2\equiv0(\mathrm{mod}\ 4)$，总之，无论 λ 和 q_k 同时是奇数还是同时是偶数，我们最后都得出 $\lambda^2+3q_k^2\equiv0(\mathrm{mod}\ 4)$，但是 $2p\equiv2(\mathrm{mod}\ 4)$，这就得出矛盾，因此不可能发生 $\lambda^2+3q_k^2=2p$ 的情况。这样 $\lambda^2+3q_k^2$ 只可能是 p 或 $3p$。

如果 $\lambda^2+3q_k^2=p$，则显然方程 $x^2+3y^2=p$ 有解。

如果 $\lambda^2+3q_k^2=3p$，则显然必有 $3\mid\lambda$，因此可设 $\lambda=3v$，因而有 $9v^2+3q_k^2=3p$，$q_k^2+3v^2=p$，因此这时方程 $x^2+3y^2=p$ 仍有解。

由引理6.7.3知有解时，当方程 $x^2+3y^2=p$ 有整数解时，本质上不同的解是唯一的。

最后，我们来研究一般的方程 $x^2+y^2=n$ 的整数解，这里 n 不再限于是素数。为此，我们首先证明以下引理：

引理6.7.5　两个平方和的积仍是一个平方和，因此有限多个平方和的积

仍是一个平方和。

证明 由恒等式$(x_1^2+y_1^2)(x_2^2+y_2^2)=(x_1x_2-y_1y_2)^2+(x_1y_2+x_2y_1)^2$即得引理。

定理 6.7.4 不定方程 $x^2+y^2=n,(x,y)=1$ 有解的充分必要条件是 $n=1,2,n_1$ 或 $2n_1$,其中

$$n_1=p_1^{a_1}p_2^{a_2}\cdots p_s^{a_s},p_i\equiv 1(\mathrm{mod}\ 4),1\leqslant i\leqslant s$$

证明 必要性:设 $x^2+y^2=n,(x,y)=1$ 有解,则由$(x,y)=1$ 和 $x^2+y^2=n$ 得出

$$(x,y)=(x,n)=(y,n)=1$$

如果 $n\equiv 0(\mathrm{mod}\ 4)$,那么由于当 x,y 一奇一偶时有$x^2+y^2\equiv 1(\mathrm{mod}\ 4)$,当 x,y 都是奇数时有$x^2+y^2\equiv 2(\mathrm{mod}\ 4)$,因而 x,y 不可能是方程$x^2+y^2=n$ 的解,因此 x,y 必须都是偶数而这又与$(x,y)=1$矛盾,所以 $n\not\equiv 0(\mathrm{mod}\ 4)$。由引理 6.7.1 可知 n 的大于 2 的素因数 p 必满足条件$\left(\frac{-1}{p}\right)=1$,即 $p\equiv 1(\mathrm{mod}\ 4)$。因此只能有 $n=1,2,n_1$ 或 $2n_1$,其中

$$n_1=p_1^{a_1}p_2^{a_2}\cdots p_s^{a_s},p_i\equiv 1(\mathrm{mod}\ 4),1\leqslant i\leqslant s$$

充分性:当 $n=1,2$ 时,方程 $x^2+y^2=n$ 显然有整数解。由定理6.7.1可知对每一个 $i,1\leqslant i\leqslant s$,方程 $x^2+y^2=p_i$ 有整数解,因此再由引理6.7.5即得方程 $x^2+y^2=n_1$ 和方程 $x^2+y^2=2n_1$ 有整数解,这就证明了充分性。

对整数 n_1,我们还可以像对于素数 $p\equiv 1(\mathrm{mod}\ 4)$ 那样用公式来求出 $x^2+y^2=n_1$ 的整数解来。由于从 $a\equiv 1(\mathrm{mod}\ 4)$ 和 $b\equiv 1(\mathrm{mod}\ 4)$ 显然可以得出 $ab\equiv 1(\mathrm{mod}\ 4)$ 来,而 n_1 的素因数全都是 $p\equiv 1(\mathrm{mod}\ 4)$ 形式的,因此显然有 $n_1\equiv 1(\mathrm{mod}\ 4)$,因而同余式

$$t^2\equiv -1(\mathrm{mod}\ n_1)$$

有解。不过这回不像在 $p\equiv 1(\mathrm{mod}\ 4)$ 时那样,只有两个解。现在有 2^s 个解,但是如果认为 t 和 $-t\equiv n_1-t(\mathrm{mod}\ n_1)$ 是本质上相同的解,则上述同余式的本质上不同的解只有 2^{s-1} 个。设$\frac{p_k}{q_k}$ 是$\frac{t}{p}$ 的满足条件$q_k<\sqrt{n_1}<q_{k+1}$ 的渐近分数,则类似于引理 6.7.4 仍然可证

$$(tq_k-pp_k)^2+q_k^2<2n_1$$

以及
$$n_1\mid(tq_k-pp_k)^2+q_k^2$$

由此得出
$$(tq_k-pp_k)^2+q_k^2=n_1$$

因而这次我们就得出了用公式求出的方程 $x^2+y^2=n_1$ 的一个解。

最后,我们还要注意,如果没有条件$(x,y)=1$,则此定理成立的条件就要改变。例如以下这些现在被排除在外的解就将被包括进来:$2^{2n}=(2^n)^2+0^2$,

$p^{2n} = (p^n)^2 + 0^2$,其中 $p \equiv 3 \pmod 4$。

为了把上述情况也包括进来,既考虑可以表为平方和的全部情况,定理 6.7.4 就需要改成

定理 6.7.5 设正整数 $n = d^2 m$,其中 m 除 1 外,没有其他的平方因数,那么不定方程

$$x^2 + y^2 = n$$

有解的充分必要条件是 $m = 1, 2, n_1$ 或 $2n_1$,其中 $n_1 = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}$。$p_i \equiv 1 \pmod 4)$,$1 \leqslant i \leqslant s$,也即 m 没有形如 $4k + 3$ 的因数。

证明的方法类似于定理 6.7.4。

说到现在,我们已弄清了在一定条件下,有些自然数是可以表示成平方和的,而另一些数则不能。但是,如果不限制加数的个数,则由

$$n = 1 + 1 + \cdots + 1 = 1^2 + 1^2 + \cdots + 1^2 (\text{共 } n \text{ 个加数})$$

就可以得出任何一个自然数都可以表示成一些正整数的平方和。于是,我们面临着以下几种可能性。

(1) 任何一个自然数 n 都可以表示成 $g(2,n)$ 个整数的平方和,这里 $g(2,n)$ 是一个依赖于 n 的自然数。并且,不存在一个不依赖于 n 的自然数 k,使得 $g(2,n) = k$。

(2) 存在一个不依赖于 n 的自然数 k,使得 $g(2,n) = k$。

在第(2) 种可能性成立时,我们还要问,最小的 k 是多少?

实际上,法国数学家拉格朗日已经否定了第(1) 种可能性,他证明了

定理 6.7.6

(1) 每一个自然数 n 必可表示成 4 个整数的平方和;

(2) 存在自然数 m,m 不可能表示成 3 个整数的平方和。

这个定理说明最小的 $k = 4$。

但是拉格朗日定理只能保证任何自然数可表示成 4 个整数的平方和,也就是说,加数可以为 0,如果要求必须表示成自然数的平方和,则可以证明:

定理 6.7.7

(1) 当 $n \geqslant 34$ 时,n 必可表示成 5 个正整数的平方和;

(2) 1,2,3,4,6,7,9,10,12,15,18,33 这 12 个数都不可能表示成 5 个正整数的平方和。

还可以提出的问题有:当一个整数可以表示成平方和时,其表示式有多少种?在不定方程 $x^2 + y^2 = n$ 有解时,其解数是多少?

类似的,还可以把上述各种问题推广到用立方和,四次方和,…,乃至 n 次方和表示数的情况。这类问题称为华林问题。到 1909 年,才有人证明,对每一个自然数 n,都存在着不依赖于 n 的最小的自然数 $g(k)$,使得 n 可以表示成 $g(k)$

个 k 次方的和。

习题 6.7

1. 将下列各数表示成平方和的形式

(1) 97 (2) 113 (3) 157 (4) 233

2. 将下列各数表示成一个平方的 2 倍与另一个平方之和的形式

(1) 41 (2) 131 (3) 193 (4) 267

3. 将下列各数表示成一个平方的 3 倍与另一个平方之和的形式

(1) 43 (2) 151 (3) 157 (4) 307

4. 求 m 为以下值时不定方程 $x^2 + y^2 = m$ 的整数解

(1) 841 (2) 3 721 (3) 5 329 (4) 2 197 (5)625

5. 求 m 为以下值时,不定方程 $x^2 + y^2 = m^2$ 的整数解

(1) 305 (2) 377 (3) 629 (4) 697

6. 求不定方程 $x^2 + y^2 = 1\ 885$ 的整数解。

7. 设 $p = x^2 + y^2$ 是素数,则 p 表为平方和的方法在不计顺序的意义下是唯一的,即如果 $p = a_1^2 + b_1^2 = a_2^2 + b_2^2, a_1 \geqslant b_1 > 0, a_2 \geqslant b_2 > 0$,则必有 $a_1 = a_2, b_1 = b_2$。

8. (1) 证明:如果 a 和 ab 都是两个整数的平方和,则 b 也是两个整数的平方和;

(2) 证明:如果 $c = m^2 + n^2, (m,n) = 1, a \geqslant 1, a \mid c$,则 $a = h^2 + k^2$, $(h,k) = 1$。

9. 证明:如果一个正整数不是两个整数的平方和,那么它也一定不是两个有理数的平方和。

10. (1) 设 $a > 0, b > 0$,则有理数 $\frac{a}{b}$ 是两个有理数的平方和的充分必要条件是 ab 是两个整数的平方和;

(2) 在(1)中如果还有 $(a,b) = 1$,则有理数 $\frac{a}{b}$ 是两个有理数的平方和的充分必要条件是 a, b 都是两个整数的平方和。

11. 设 $p > 3$ 是素数。证明:当且仅当 $p \equiv 1 \pmod 6$ 时,不定方程 $x^2 - xy + y^2 = p$ 有解。

12. 证明:$n = 2 \cdot 4^a (a \geqslant 0)$ 不可能表示成 4 个正整数的平方和。

13. (1) 证明:1,2,3,4,6,7,9,10,12,15,18,33 这 12 个数都不可能表示成 5 个正整数的平方和;

(2) 通过直接验证当 $n \leqslant 168$ 且不等于(1)中所给的 12 个数时,n 必可表示成 5 个正整数的平方和;

(3) 验证

$$
\begin{aligned}
169 = {} & 10^2 + 6^2 + 4^2 + 4^2 + 1^2 = \\
& 11^2 + 4^2 + 4^2 + 4^2 = \\
& 12^2 + 4^2 + 3^2 = \\
& 12^2 + 5^2 = \\
& 13^2
\end{aligned}
$$

(4) 利用拉格朗日定理(定理 6.7.5) 和(3) 证明每一个大于等于 169 的自然数都可以表示成 5 个正整数的平方和;

(5) 利用(2),(4) 证明每一个大于等于 34 的自然数都可以表示成 5 个正整数的平方和;

(6) 设 $g(k)$ 是任意一个不依赖于 n 而只依赖于 k 的大于 1 的整数值函数。证明:不可能把每个自然数都表示成 $g(k)$ 个 k 次方的和。

14. 证明:$2^k(k \geqslant 0)$ 不可能表示成 3 个正整数的平方和,并直接求出 $x_1^2 + x_2^2 + x_3^2 + x_4^2 = 2^k$ 的所有解。

15. (1) 证明:有无穷多个 n 使得 $x_1^2 + x_2^2 + x_3^2 + x_4^2 = n$ 不存在满足条件 $(x_1, x_2, x_3, x_4) = 1$ 的解;

(2) 证明:有无穷多个 n 使得 $x_1^2 + x_2^2 + x_3^2 + x_4^2 = n$ 不存在满足条件 $x_1 > x_2 > x_3 > x_4 \geqslant 0$ 的解。

第七章 用有理数逼近实数

在这一章中，我们要专门讨论关于用有理数去逼近实数的问题。这个问题之所以重要，是由于我们在实际计算中只能对有理数进行精确的计算操作，任何涉及实数的计算实际上都先要把实数换成它的有理近似值才能进行。

最简单的逼近方法就是把实数化成小数，然后把无限小数截断成有限小数。然而这样所得的逼近往往不是最好的。

说到这里，就产生了一个什么叫“好”的逼近的问题，粗略地讲，在满足一定误差要求下，如果用来逼近实数的有理数的分母越小，就认为这个逼近越好，因为分母小的有理数一般就认为是比较简单的分数，能用比较简单的分数来逼近一个数，当然就认为这样的逼近是“好”的。

给了一个实数 θ 和一个有理数$\frac{p}{q}$，我们可以用$\left|\theta-\frac{p}{q}\right|$来描述$\theta$和$\frac{p}{q}$之间的误差，也可以用$|q\theta-p|$来描述$\theta$和$\frac{p}{q}$之间的误差，这样就产生了两类逼近问题，第一类用$\left|\theta-\frac{p}{q}\right|$作为误差，第二类用$|q\theta-p|$作为误差，这两类逼近问题既有联系也有区别。

现在我们介绍第一个属于第二类逼近的引理。

引理 7.1　任给实数 θ 和正整数 N，必存在整数 h 和 k 使得

$$0 < k \leqslant N$$

而

$$|k\theta - h| < \frac{1}{N}$$

证明　令 $\{x\} = x - [x]$ 表示 x 的分数部分。考虑 $N+1$ 个实数 $0, \{\theta\}, \{2\theta\}, \cdots, \{N\theta\}$。所有这些数都位于半开区间 $[0,1]$ 中，并把此开区间分成了 N 个长度都是 $\frac{1}{N}$ 的半开子区间（每个半开子区间都包含其左端的端点）。因此，必有某一个半开子区间包含至少两个数。不妨设其为 $\{a\theta\}$ 和 $\{b\theta\}$，其中 $0 \leqslant a < b \leqslant N$，因此

$$|\{b\theta\} - \{a\theta\}| < \frac{1}{N}$$

但

$$\{b\theta\} - \{a\theta\} = b\theta - [b\theta] - (a\theta - [a\theta]) = (b-a)\theta - ([b\theta] - [a\theta])$$

令

$$k = b - a, h = [b\theta] - [a\theta]$$

则上面的不等式就成为

$$|k\theta - h| < \frac{1}{N}, 0 < k \leqslant N$$

这就证明了引理。

上面这个引理只说存在着整数 h 和 k 具有引理所说的性质，但并没有说 h 和 k 一定是互素的，这在很多情况下应用这个引理时会让人感到不方便，我们可以对此作一些改进。

引理 7.2　任给实数 θ 和正整数 N，必存在互素的整数 h 和 k 使得

$$0 < k \leqslant N$$

而

$$|k\theta - h| < \frac{1}{N}$$

证明　由引理 7.1，存在整数 h' 和 k' 使得 $0 < k' \leqslant N$ 而

$$|k'\theta - h'| < \frac{1}{N}$$

或者

$$\left|\theta - \frac{h'}{k'}\right| < \frac{1}{k'N}$$

设 $(h', k') = d$。如果 $d = 1$，那么引理已经成立。如果 $d > 1$，那么 $h' = dh$，$k' = dk$，而 $(h,k) = 1$。而且 $0 < k < k' \leqslant N$，因而 $\frac{1}{k'} < \frac{1}{k}$。因此上面的不等式现在成为

$$\left|\theta - \frac{h}{k}\right| < \frac{1}{k'N} < \frac{1}{kN}$$

由此即得

$$|k\theta - h| < \frac{1}{N}$$

且 $0 < k \leqslant N$，h 和 k 互素。这就证明了引理。

定理 7.1(迪利克雷逼近) 任给实数 θ，那么必存在整数 h 和 k 使得 $k > 0$，$(h,k) = 1$，而

$$\left| \theta - \frac{h}{k} \right| < \frac{1}{k^2}$$

迪利克雷(Dirichlet, Peter Gustav Lejeune, 1805—1859)，德国数学家．生于迪伦，卒于格丁根．

证明 由引理 7.2 知必存在整数 h 和 k 使得 $k > 0$，$(h,k) = 1$，$0 < k \leqslant N$ 而

$$\left| \theta - \frac{h}{k} \right| < \frac{1}{kN} \leqslant \frac{1}{k^2}$$

这就证明了引理。

下面我们对什么是"好"的逼近给出确切的定义。

定义 7.1 称分数 $\frac{a}{b}(b > 0)$ 是实数 θ 的第一类最佳逼近，如果任何分母不超过 b 的其他分数 $\frac{c}{d}$ 与 θ 的误差都大于 $\frac{a}{b}$ 与 θ 的误差。也就是说，如果 $0 < d \leqslant b$，$\frac{c}{d} \neq \frac{a}{b}$，则必有

$$\left| \theta - \frac{c}{d} \right| > \left| \theta - \frac{a}{b} \right|$$

下面的主要问题就是研究什么样的数才能是实数 θ 的最佳逼近。

定义 7.2 设 $b > 0$，$d > 0$，则称分数 $\frac{a+c}{b+d}$ 为分数 $\frac{a}{b}$ 与 $\frac{c}{d}$ 的中位数。

引理 7.3 两个分数的中位数必介于这两个分数之间。

证明 设给出的两个分数为 $\frac{a}{b}$ 和 $\frac{c}{d}$，$b > 0$，$d > 0$，那么必有 $\frac{a}{b} \leqslant \frac{c}{d}$ 或 $\frac{a}{b} \geqslant \frac{c}{d}$。为确定起见，不妨设 $\frac{a}{b} \leqslant \frac{c}{d}$，那么 $bc - ad \geqslant 0$，于是

$$\frac{a+c}{b+d} - \frac{a}{b} = \frac{bc-ad}{b(b+d)} \geqslant 0, \frac{c}{d} - \frac{a+c}{b+d} = \frac{bc-ad}{d(b+d)} \geqslant 0$$

因此

$$\frac{a}{b} \leqslant \frac{a+c}{b+d} \leqslant \frac{c}{d}$$

同理可证 $\frac{a}{b} \geqslant \frac{c}{d}$ 的情况。

设 $\frac{p_k}{q_k}$ 是实数 θ 的渐近分数，那么

$$\frac{p_{k-1}(i+1)+p_{k-2}}{q_{k-1}(i+1)+q_{k-2}} - \frac{p_{k-1}i+p_{k-2}}{q_{k-1}i+q_{k-2}} = \frac{(-1)^k}{(q_{k-1}(i+1)+q_{k-2})(q_{k-1}i+q_{k-2})}$$

由此看出上面的差数的符号，当 k 固定时与 i 无关，或者对所有的 $i \geqslant 0$，这些差的符号不变。它们的符号只与 k 的奇偶性有关，由此可见有

引理 7.4 当 k 为偶数时，分数叙列

$$\frac{p_{k-2}}{q_{k-2}},\frac{p_{k-2}+p_{k-1}}{q_{k-2}+q_{k-1}},\frac{p_{k-2}+2p_{k-1}}{q_{k-2}+2q_{k-1}},\cdots,\frac{p_{k-2}+a_kp_{k-1}}{q_{k-2}+a_kq_{k-1}}=\frac{p_k}{q_k}$$

是递增的，而当 k 为奇数时，是递减的。

定义 7.3 设$\frac{p_{k-2}}{p_{k-2}}$和$\frac{p_k}{q_k}$是实数θ的两个阶数相差为2、奇偶性相同的渐近分数，则位于叙列

$$\frac{p_{k-2}}{q_{k-2}},\frac{p_{k-2}+p_{k-1}}{q_{k-2}+q_{k-1}},\frac{p_{k-2}+2p_{k-1}}{q_{k-2}+2q_{k-1}},\cdots,\frac{p_{k-2}+a_kp_{k-1}}{q_{k-2}+a_kq_{k-1}}=\frac{p_k}{q_k}$$

两端之间的那些中间项(如果它们存在，即 $a_k>1$ 时)就称为是位于渐近分数$\frac{p_{k-2}}{q_{k-2}}$和$\frac{p_k}{q_k}$之间的中间分数。

引理 7.5 设$\frac{p_k}{q_k}$是实数θ的渐近分数，则

(1) 当 k 是偶数时，$\frac{p_{k-2}}{q_{k-2}}<\frac{p_{k-2}+p_{k-1}}{q_{k-2}+q_{k-1}}<\cdots<\frac{p_k}{q_k}<\theta<\frac{p_{k-1}}{q_{k-1}}$;

(2) 当 k 是奇数时，$\frac{p_{k-2}}{q_{k-2}}>\frac{p_{k-2}+p_{k-1}}{q_{k-2}+q_{k-1}}>\cdots>\frac{p_k}{q_k}>\theta>\frac{p_{k-1}}{q_{k-1}}$。

特别地，一个数θ总是介于其任一个渐近分数及此渐近分数与其前一个渐近分数的中位数之间。

证明 由定理 6.2.1 的证明可知

$$\theta_1>\theta_3>\cdots>\theta_{2n-1}>\cdots>\theta>\cdots>\theta_{2n}>\cdots\theta_2>\theta_0$$

其中 $\theta_k=\frac{p_k}{q_k}$ 表示θ的第k阶渐近分数。再由引理 7.4 即得到引理 7.5。

现在我们来证明

定理 7.2 实数θ的任意第一类最佳逼近必是θ的渐近分数或中间分数(约定 $p_{-1}=1,q_{-1}=0$)。

证明 设$\frac{a}{b}(b>0)$是θ的第一类最佳逼近。$\theta=[a_0;a_1,a_2,\cdots]$，则由于 $a_0=[\theta]$，因此 $0\leqslant\theta-a_0<1$。这时不可能$\frac{a}{b}<a_0$，否则$0\leqslant\theta-a_0<\theta-\frac{a}{b}$，因而$\left|\theta-\frac{a_0}{1}\right|<\left|\theta-\frac{a}{b}\right|$。

由于$1\leqslant b$，因此如果$\frac{a}{b}\neq a_0=\frac{a_0}{1}$，那么上述不等式就与$\frac{a}{b}$是$\theta$的第一类最佳逼近的假设相矛盾。这样由$\frac{a}{b}<a_0$就必须导出$\frac{a}{b}=a_0$，这又导出矛盾。

也不可能$\frac{a}{b}>a_0+1$，否则将有$\frac{a}{b}-\theta>a_0+1-\theta>0$，因而$\left|\theta-\frac{a_0+1}{1}\right|<$

$\left|\theta-\frac{a}{b}\right|$。与上面的论述类似，无论$\frac{a}{b}$是否等于$a_0+1$都将导出矛盾，因此必有

$$a_0 \leqslant \frac{a}{b} \leqslant a_0+1$$

如果$\frac{a}{b}=a_0$，则由于$a_0=\frac{a_0}{1}=\frac{p_0}{q_0}$，因此定理的结论这时已经成立。

如果$\frac{a}{b}=a_0+1$，则由于

$$a_0+1=\frac{a_0+1}{1}=\frac{p_0+p_{-1}}{q_0+q_{-1}}$$

因此定理的结论这时也已经成立。

故以下不妨设

$$a_0 < \frac{a}{b} < a_0+1$$

如果$\frac{a}{b}$既不等于θ的渐近分数也不等于θ的中间分数，那么$\frac{a}{b}$必然位于某个叙列

$$\frac{p_{k-2}}{q_{k-2}},\frac{p_{k-2}+p_{k-1}}{q_{k-2}+q_{k-1}},\frac{p_{k-2}+2p_{k-1}}{q_{k-2}+2q_{k-1}},\cdots,\frac{p_{k-2}+a_kp_{k-1}}{q_{k-2}+a_kq_{k-1}}=\frac{p_k}{q_k}$$

中的某两个数之间，因此存在整数k和r使得$k>0,0\leqslant r<a_{k+1}$（当$r=a_{k+1}$时，$\frac{p_kr+p_{k-1}}{q_kr+q_{k-1}}=\frac{p_{k+1}}{q_{k+1}}$已经是一个渐近分数了）或者$k=0,1\leqslant r<a_1$（当$k=0$时，$r$不能等于0，否则$\frac{p_kr+p_{k-1}}{q_kr+q_{k-1}}=\frac{p_{-1}}{q_{-1}}=\frac{1}{0}$，这不可能。如果$r=a_1$，则$\frac{p_kr+p_{k-1}}{q_kr+q_{k-1}}=\frac{p_1}{q_1}$也已经是一个渐近分数了），而$\frac{a}{b}$位于$\frac{p_kr+p_{k-1}}{q_kr+q_{k-1}}$和$\frac{p_k(r+1)+p_{k-1}}{q_k(r+1)+q_{k-1}}$之间，因此

$$\left|\frac{a}{b}-\frac{p_kr+p_{k-1}}{q_kr+q_{k-1}}\right|<\left|\frac{p_k(r+1)+p_{k-1}}{q_k(r+1)+q_{k-1}}-\frac{p_kr+p_{k-1}}{q_kr+q_{k-1}}\right|=\frac{1}{(q_k(r+1)+q_{k-1})(q_kr+q_{k-1})}$$

但是
$$\left|\frac{a}{b}-\frac{p_kr+p_{k-1}}{q_kr+q_{k-1}}\right|=\frac{m}{b(q_kr+q_{k-1})}$$

其中$m\geqslant 1$，因而

$$\frac{1}{b(q_kr+q_{k-1})}\leqslant\frac{m}{b(q_kr+q_{k-1})}<\frac{1}{(q_k(r+1)+q_{k-1})(q_kr+q_{k-1})}$$

由此得出

$$q_k(r+1)+q_{k-1}<b$$

但是由引理 7.5 可知分数 $\xi_{r+1}=\dfrac{p_k(r+1)+p_{k-1}}{q_k(r+1)+q_{k-1}}$ 比分数 $\xi_r=\dfrac{p_kr+p_{k-1}}{q_kr+q_{k-1}}$ 更接近于 θ。由于 $\dfrac{a}{b}$ 位于 ξ_r 和 ξ_{r+1} 之间，故分数 ξ_{r+1} 比 $\dfrac{a}{b}$ 更接近于 θ，但由上面已证的不等式 $q_k(r+1)+q_{k-1}<b$ 可知 ξ_{r+1} 的分母比 $\dfrac{a}{b}$ 的分母小，这与 $\dfrac{a}{b}$ 是 θ 的第一类最佳逼近的假设相矛盾，所得的矛盾便证明了定理的结论。

现在考虑所谓的第二类最佳逼近问题。

定义 7.4 称分数 $\dfrac{a}{b}(b>0)$ 是实数 θ 的第二类最佳逼近，如果由 $\dfrac{c}{d}\neq\dfrac{a}{b}(0<d\leqslant b)$ 可以得出

$$|d\theta-c|>|b\theta-a|$$

引理 7.6 第二类最佳逼近一定是第一类最佳逼近，但反过来的结论不成立。

证明 设 $\dfrac{a}{b}$ 是实数 θ 的第二类最佳逼近，但不是第一类最佳逼近，则由第一类最佳逼近的定义必存在分数 $\dfrac{c}{d}(0<d\leqslant b)$ 而 $\left|\theta-\dfrac{c}{d}\right|\leqslant\left|\theta-\dfrac{a}{b}\right|$。用 $d<b$ 和这个不等式相乘(相乘之后，不等式不变号)得到 $|d\theta-c|\leqslant|b\theta-a|$。这与 $\dfrac{a}{b}$ 是实数 θ 的第二类最佳逼近的假设相矛盾。这就证明了第二类最佳逼近一定也是第一类最佳逼近。

设 $\theta=\dfrac{1}{5}$，$\dfrac{a}{b}=\dfrac{1}{3}$。我们证 $\dfrac{a}{b}$ 是 θ 的第一类最佳逼近。如果 $\dfrac{1}{3}$ 不是 θ 的第一类最佳逼近，则存在分数 $\dfrac{c}{d}$ 满足条件 $0<d\leqslant3$，$\dfrac{c}{d}\neq\dfrac{1}{3}$，而

$$\left|\frac{c}{d}-\frac{1}{5}\right|\leqslant\left|\frac{1}{3}-\frac{1}{5}\right|=\frac{2}{15}$$

由此得出

$$\frac{1}{15}\leqslant\frac{c}{d}\leqslant\frac{5}{15}=\frac{1}{3}$$

故
$$0<d\leqslant15c\leqslant5d\leqslant15$$

这又得出 $0<c\leqslant1$，故 $c=1$。把 $c=1$ 代入上式又得出 $d\geqslant3$。但又有 $0<d\leqslant3$，因此 $d=3$。这样最后就得出 $\dfrac{c}{d}=\dfrac{1}{3}$。这与 $\dfrac{c}{d}\neq\dfrac{1}{3}$ 的假设矛盾，所得的矛盾就说明 $\dfrac{a}{b}=\dfrac{1}{3}$ 必是 θ 的第一类最佳逼近。

但是如果取 $\dfrac{c}{d}=\dfrac{0}{1}$，则 $\dfrac{c}{d}\neq\dfrac{1}{3}=\dfrac{a}{b}$，$0<d<3=b$，而

$$|d\theta - c| = \left|1 \cdot \frac{1}{5} - 0\right| = \frac{1}{5} < \frac{2}{5} = \left|3\frac{1}{5} - 1\right| = |b\theta - a|$$

这就说明$\frac{a}{b} = \frac{1}{3}$不是$\theta$的第二类最佳逼近。

由此可见第二类最佳逼近是比第一类最佳逼近更好的逼近。从定理7.2我们知道，实数θ的任意第一类最佳逼近必是θ的渐近分数或中间分数（约定$p_{-1} = 1, q_{-1} = 0$）。因此第二类最佳逼近也必是θ的渐近分数或中间分数。下面我们证明第二类最佳逼近只可能是θ的渐近分数。

定理7.3　实数θ的任意第二类最佳逼近只可能是θ的渐近分数。

证明　设$r = \frac{a}{b}(b > 0)$是θ的第二类最佳逼近。$\theta = [a_0; a_1, a_2, \cdots]$，则必有

$$0 < \theta - a_0 < 1, 0 < \theta - a_0 = \frac{1}{a_1 + \cdots} < 1$$

$$a_0 \leqslant r \leqslant a_0 + 1$$

因为在相反的情况下，即$r < a_0$或$r > a_0 + 1$的情况下，由定理7.2的证明可知r不可能是θ的第一类最佳逼近，故由引理7.6知r更不可能是θ的第二类最佳逼近，而这与假设矛盾。

设$\theta_k = \frac{p_k}{q_k}$表示$\theta$的第$k$阶渐近分数，则由定理6.2.1的证明可知

$$\theta_1 > \theta_3 > \cdots > \theta_{2n-1} > \cdots > \theta > \cdots > \theta_{2n} > \cdots\theta_2 > a_0$$

如果r不等于θ的任何渐近分数，则由上式可知只可能发生以下三种情况之一：

(1) $r > \theta_1 > \theta$;

(2) $\theta > r > \theta_0$;

(3) 对某个n，r位于θ_{n-1}与θ_{n+1}之间，或更确切地说，又有可能发生以下两种情况之一：

(i) $\theta_n < \theta < \theta_{n+1} < r = \frac{a}{b} < \theta_{n-1}$;

(ii) $\theta_{n-1} < r = \frac{a}{b} < \theta_{n+1} < \theta < \theta_n$。

如果发生情况(1)，则

$$\left|\theta - \frac{a}{b}\right| = |\theta - r| = |r - \theta_1| + |\theta - \theta_1| > |\theta_1 - r| = \left|\frac{p_1}{q_1} - \frac{a}{b}\right| \geqslant \frac{1}{bq_1}$$

由此得出

$$|b\theta - a| > \frac{1}{q_1} = \frac{1}{a_1}$$

但是又有

$$|\theta - a_0| = \theta - a_0 = \frac{1}{a_1 + \cdots} \leqslant \frac{1}{a_1}$$

故
$$|1 \cdot \theta - a_0| \leqslant \frac{1}{a_1} < |b\theta - a|, 1 \leqslant b$$

而这与 r 是 θ 的第二类最佳逼近的假设相矛盾。因此情况(1) 不可能发生。

同理可以证明情况(2) 不可能发生。

如果发生情况(3),则

$$|r - \theta_{n-1}| = \left|\frac{a}{b} - \frac{p_{n-1}}{q_{n-1}}\right| \geqslant \frac{1}{bq_{n-1}}$$

另一方面,无论发生情况(1) 还是情况(2),都会得出 r 位于 θ_{n-1} 和 θ_n 之间的结论,因此

$$|r - \theta_{n-1}| < |\theta_n - \theta_{n-1}| = \left|\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}}\right| = \frac{1}{q_n q_{n-1}}$$

$$\frac{1}{bq_{n-1}} \leqslant |r - \theta_{n-1}| < \frac{1}{q_n q_{n-1}}$$

故必有

$$q_n < b$$

由

$$|\theta - \theta_{n+1}| + |\theta_{n+1} - r| = |\theta - r|$$

知
$$\left|\theta - \frac{a}{b}\right| = |\theta - r| \geqslant |\theta_{n+1} - r| = \left|\frac{p_{n+1}}{q_{n+1}} - \frac{a}{b}\right| \geqslant \frac{1}{bq_{n+1}}$$

由此得出

$$|b\theta - a| \geqslant \frac{1}{q_{n+1}}$$

而由定理 6.2.2 又有

$$\left|\theta - \frac{p_n}{q_n}\right| < \frac{1}{q_n q_{n+1}}$$

因此
$$|q_n\theta - p_n| < \frac{1}{q_{n+1}} \leqslant |b\theta - a|$$

但是 $q_n < b$ 说明 r 不是 θ 的第二类最佳逼近,这与假设矛盾,因此情况(3) 也不可能发生。由于情况(1),(2),(3) 都不可能发生,因此 r 只能是 θ 的渐近分数。

上面我们已经证明了实数 θ 的任意第一类最佳逼近必是 θ 的渐近分数或中间分数(约定 $p_{-1} = 1, q_{-1} = 0$)。而第二类最佳逼近只可能是 θ 的渐近分数。现在我们来考虑反过来的问题,即哪些分数才能是实数 θ 的第一类最佳逼近或第二类最佳逼近的问题。

引理 7.7 设 θ 是任意实数, $c > 1$ 是一个正数, x, y 是整数,令

$$m = \inf_{0<y\leqslant c} |y\theta - x|$$

则
$$m = \min_{0<y\leqslant c} |y\theta - x|$$

证明 设 $\Omega(\theta,c) = \{x \mid |y\theta - x| = m\}$，$0 < y_0 < c$，$x \in \Omega(\theta,c)$，$0 < y \leqslant c$，则由下确界及绝对值的不等式可以得出

$$|x| - y|\theta| \leqslant |y\theta - x| \leqslant |y_0\theta - 1| \leqslant y_0|\theta| + 1$$

故
$$|x| \leqslant y_0|\theta| + 1 + y|\theta| \leqslant (y_0 + c)|\theta| + 1 \leqslant 2c|\theta| + 1$$

这表明如果 $x \in \Omega(\theta,c)$，$0 < y \leqslant c$，则 x 是有界的。因此适合 $x \in \Omega(\theta,c)$，$0 < y \leqslant c$ 的整数对 (x,y) 也是有限集，因而

$$m = \min_{0<y\leqslant c} |y\theta - x|$$

引理7.8 设 θ 是任意实数，$\theta \neq [\theta] + \dfrac{1}{2}$，$c > 1$ 是一个正数，x,y 是整数。

$$m = \inf_{0<y\leqslant c} |y\theta - x|, \Omega(\theta,c) = \{x \mid |y\theta - x| = m\}$$

$$y_0 = \min\{y \mid |y\theta - x| = m\}$$

则存在唯一的 x_0 使得 $x_0 \in \Omega(\theta,c) = \{x \mid |y\theta - x| = m\}$ 或唯一的 x_0 使得

$$|y_0\theta - x_0| = m = \inf_{0<y\leqslant c} |y\theta - x|$$

证明 由引理7.7知 m 是可以达到的，即存在 (x_0,y_0) 使得

$$|y_0\theta - x_0| = m = \inf_{0<y\leqslant c} |y\theta - x|$$

设 x_0 不唯一，即存在 $x'_0 \neq x_0$，而

$$|y_0\theta - x_0| = |y_0\theta - x'_0| = m$$

则
$$y_0\theta - x_0 = y_0\theta - x'_0$$

或者
$$y_0\theta - x_0 = -(y_0\theta - x'_0)$$

但由
$$y_0\theta - x_0 = y_0\theta - x'_0$$

得出 $x'_0 = x_0$ 与假设矛盾，因此只能

$$y_0\theta - x_0 = -(y_0\theta - x'_0)$$

因而

$$\theta = \frac{x_0 + x'_0}{2y_0} \neq \frac{x_0}{y_0}\text{（因为由}\frac{x_0 + x'_0}{2y_0} = \frac{x_0}{y_0}\text{我们再次得出 } x'_0 = x_0 \text{ 的矛盾）}$$

我们证明分数 θ 不可约。假设不然，则必有

$$x_0 + x'_0 = ta, 2y_0 = tb, t > 0, \theta = \frac{a}{b}$$

如果 $t > 2$，则 $0 < b < y_0$，$|b\theta - a| = 0$，这与 y_0 的定义矛盾，故不可能。

如果 $t = 2$，则 $y_0 = b$，$y_0\theta - x_0 \neq 0$（由于 $\theta = \dfrac{x_0 + x'_0}{2y_0} \neq \dfrac{x_0}{y_0}$），故

$$|b\theta - a| = |y_0\theta - a| = 0 < |y_0\theta - x_0|$$

这说明 $x_0 \notin \Omega(\theta, c) = \{x \mid |y\theta - x| = m\}$，因而与$(x_0, y_0)$的定义矛盾。

因此 t 只能等于1，这就说明 θ 是不可约的。现将 θ 表示成连分数，由于 θ 是有理数，因此

$$\theta = \frac{p_n}{q_n} = \frac{x_0 + x'_0}{2y_0}$$

而由于$\frac{p_n}{q_n}$和$\frac{x_0 + x'_0}{2y_0}$都不可约，因此由上式就得出

$$p_n = x_0 + x'_0$$

$$q_n = 2y_0 = a_n q_{n-1} + q_{n-2}, a \geqslant 2$$

（注意，按照我们的约定，一个有限简单连分数的最后一个元素不为1，因此 $a_n \geqslant 2$）。

如果 $n = 1, a_n = 2$，则 $\theta = [\theta] + \frac{1}{2}$，与假设不合。故只可能 $n > 1, a_n = 2$ 或 $n = 1, a_n > 2$。

在 $n = 1, a_n > 2$ 的情况下

$$q_{n-1} = \frac{2y_0 - q_{n-2}}{a_n} \leqslant \frac{2y_0}{a_n} < y_0$$

在 $n > 1, a_n = 2$ 的情况下

$$q_{n-1} = \frac{2y_0 - q_{n-2}}{2} = y_0 - \frac{q_{n-2}}{2} < y_0$$

因此无论发生哪种情况都有 $0 < q_{n-1} < y_0$。

但是另一方面

$$|q_{n-1}\theta - p_{n-1}| = q_{n-1}\left|\theta - \frac{p_{n-1}}{q_{n-1}}\right| = q_{n-1}\left|\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}}\right| = q_{n-1}\frac{1}{q_n q_{n-1}} = \frac{1}{q_n}$$

（定理6.1.2）故

$$|q_{n-1}\theta - p_{n-1}| = \frac{1}{q_n} = \frac{1}{2y_0} \leqslant \frac{1}{2} \leqslant \left|\frac{x'_0 - x_0}{2}\right| = |y_0\theta - x_0|$$

而这与(x_0, y_0)的定义相矛盾，所得的矛盾便证明了对 y_0，存在唯一的 x_0 使得 $x_0 \in \Omega(\theta, c) = \{x \mid |y\theta - x| = m\}$ 或唯一 x_0 的使得

$$|y_0\theta - x_0| = m = \inf_{0<y\leqslant c} |y\theta - x|$$

引理7.9　设 θ 是任意实数，$c > 1$ 是一个正数，x, y 是整数。$m = \inf\limits_{0<y\leqslant c} |y\theta - x|$。$(x_0, y_0)$ 使得 $0 < y_0 \leqslant c$，$|y_0\theta - x_0| = m = \inf\limits_{0<y\leqslant c} |y\theta - x|$。

则$\frac{x_0}{y_0}$必是 θ 的第二类最佳逼近。

证明　设$\frac{a}{b} \neq \frac{x_0}{y_0}$，$0 < b \leqslant y_0$。在引理7.8中，我们已经证明如果 θ 是任

意实数，$c>1$是一个正数，x,y是整数。$m=\inf\limits_{0<y\leqslant c}|y\theta-x|$。$(x_0,y_0)$使得$0<y_0\leqslant c$，$|y_0\theta-x_0|=m=\inf\limits_{0<y\leqslant c}|y\theta-x|$，则$(x_0,y_0)$是唯一的。

因此如果$|b\theta-a|\leqslant|y_0\theta-x_0|$，则由$(x_0,y_0)$的唯一性就得出$x_0=a$，$y_0=b$，从而$\frac{a}{b}=\frac{x_0}{y_0}$，这与假设矛盾。这就说明必有$|b\theta-a|>|y_0\theta-x_0|$，这也就是说$\frac{x_0}{y_0}$必是$\theta$的第二类最佳逼近。

定理 7.4 设θ是任意实数，$\theta_n=\frac{p_n}{q_n}$是θ的第n阶渐近分数，则$\theta_n=\frac{p_n}{q_n}$ $(n\geqslant 1)$都是θ的第二类渐进逼近。

证明 如果$\theta=[\theta]+\frac{1}{2}$，则$\theta=\theta_1=\frac{p_1}{q_1}$，因此显然$\theta_1=\frac{p_1}{q_1}$是$\theta$的第二类渐进逼近。

如果$\theta\neq[\theta]+\frac{1}{2}$，则由引理 7.8 知存在唯一的$(x_{n0},y_{n0})$使得

$$y_{n0}=\min\{y\mid x\in\Omega(\theta,q_n)\}$$

$$|y_{n0}\theta-x_{n0}|=m_n=\inf_{0<y\leqslant q_n}|y\theta-x|,n\geqslant 1$$

同时由引理 7.9 又知$\frac{x_{n0}}{y_{n0}}$必是θ的第二类渐进逼近，因而再由定理 7.3 知$\frac{x_{n0}}{y_{n0}}$必是θ的某一渐近分数$\theta_k=\frac{p_k}{q_k}$。由连分数的性质(定理6.2.2)知$\theta_{k+1}=\frac{p_{k+1}}{q_{k+1}}$要比$\theta_k=\frac{p_k}{q_k}$更接近$\theta$，因而由$y_{n_0}$的定义知必有$k\leqslant n$。

我们证不可能有$k<n$，否则由定理 6.2.2 就有

$$\frac{1}{q_{n-1}+q_n}\leqslant\frac{1}{q_{k+1}+q_k}<|q_k\theta-p_k|=|y_{n0}\theta-x_{n0}|\leqslant|q_n\theta-p_n|\leqslant\frac{1}{q_{n+1}}$$

由此得出

$$q_{n+1}<q_n+q_{n-1}$$

但上式与$q_{n+1}=a_{n+1}q_n+q_{n-1}\geqslant q_n+q_{n-1}$相矛盾。从而必有$k=n\geqslant 1$，即$\theta_n=\frac{p_n}{q_n}=\frac{x_{n0}}{y_{n0}}$是$\theta$的第二类最佳逼近。

总结上面的结果可以看出，连分数在迪利克雷逼近问题中起了非常重要的作用。对迪利克雷逼近问题我们引进了两种用来度量逼近程度的“好”的标准：第一类最佳逼近和第二类最佳逼近的概念，结果我们证明了，任何第一类最佳逼近只能是连分数或中间分数，而任何第二类最佳逼近只能是连分数，反过来，任何大于 1 阶的渐近分数必然都是第二类最佳逼近，从而也是第一类最佳逼近。

上面的结果已经解决了迪利克雷逼近问题有解的问题。下面我们来考虑关

于迪利克雷逼近问题的更深入的问题，即逼近的阶和逼近的常数问题。

为了估计误差 $\left|\theta-\frac{a}{b}\right|$ 的大小，一个自然的方法是用有理数 $\frac{a}{b}$ 的分母 b 作标准，去寻找一个 b 的函数（显然只能考虑 b 的减函数，否则逼近的结果的估计只能越来越"坏"）$f(b)$，使得 $\left|\theta-\frac{a}{b}\right|<f(b)$ 有无穷多组解。由定理 6.2.2 知 $\left|\theta-\frac{p_k}{q_k}\right|<\frac{1}{q_k^2}$。这说明逼近问题 $\left|\theta-\frac{a}{b}\right|<\frac{1}{b^2}$ 有无穷多组解，或者说我们可以用有理数对任意实数做阶为 $\frac{1}{b^2}$ 级的逼近。因此，首先引起兴趣的一个问题是，上述逼近在阶和常数两方面是否可以进一步改进？即是否可以得到比 $\frac{1}{b^2}$ 更高阶的逼近？或者是否可以得到 $\frac{C}{b^2}$，$0<C<1$ 类型的逼近？回答是如果要求寻找对任意实数和所有满足迪利克雷逼近问题的有理数（实际上，只须考虑满足最佳逼近的有理数，因为其他的有理数的逼近程度更差）都适用的函数，则无论逼近的阶还是常数都不可能再改进。

例如，设 $\theta=\frac{\sqrt{5}+1}{2}$，则易于证明 θ 的第 n 个渐进分数为 $\frac{F_{n+2}}{F_{n+1}}$，其中 F_n 满足 $F_1=F_2=1, F_n=F_{n-1}+F_{n-2}$ 是所谓的斐波那契数，因此由定理 6.2.2 得出

$$F_{n+3}=F_{n+2}+F_{n+1}=2F_{n+1}+F_n<3F_{n+1}$$

$$3F_{n+1}^2>F_{n+1}F_{n+3}$$

$$\left|\theta-\frac{F_{n+2}}{F_{n+1}}\right|\geqslant\frac{1}{F_{n+1}(F_{n+1}+F_{n+2})}=\frac{1}{F_{n+1}F_{n+3}}>\frac{1}{3F_{n+1}^2}$$

这说明对 $\theta=\frac{\sqrt{5}+1}{2}$ 来说，不可能得到比 $\frac{1}{b^2}$ 更高阶的逼近。

再考虑 $\theta=[0;n,1,n]=\frac{n+1}{n(n+2)}$，对于这个数，$p_1=1, q_1=n, p_3=n+1, q_3=n(n+2)$。因此

$$\left|\theta-\frac{p_1}{q_1}\right|=\left|\frac{p_3}{q_3}-\frac{p_1}{q_1}\right|=\frac{1}{n(n+2)}=\frac{1}{\left(1+\frac{2}{n}\right)q_1^2}$$

因此，任给 $\epsilon>0$，我们总可以找到一个 n，使得 $\frac{1}{1+\frac{2}{n}}>1-\epsilon$。因此

$$\left|\theta-\frac{p_1}{q_1}\right|>\frac{1-\epsilon}{q_1^2}$$

这表明逼近的常数也不可能改善。

但是如果放弃对所有满足逼近问题的有理数都适用这一要求，则又可以得

到许多有趣而又重要的结果。

定理 7.5 如果 θ 存在第 $n(n>0)$ 阶渐近分数，则在不等式

$$\left|\theta-\frac{p_{n-1}}{q_{n-1}}\right|<\frac{1}{2q_{n-1}^2} \text{和} \left|\theta-\frac{p_n}{q_n}\right|<\frac{1}{2q_n^2}$$

之中，至少有一个成立。

证明 由于 θ 必位于$\frac{p_{n-1}}{q_{n-1}}$和$\frac{p_n}{q_n}$之间，故有

$$\left|\theta-\frac{p_{n-1}}{q_{n-1}}\right|+\left|\theta-\frac{p_n}{q_n}\right|=\left|\frac{p_n}{q_n}-\frac{p_{n-1}}{q_{n-1}}\right|=\frac{1}{q_nq_{n-1}}<\frac{1}{2q_{n-1}^2}+\frac{1}{2q_n^2}$$

（这里应用了当 $a\neq b, a>0, b>0$ 时，$2ab<a^2+b^2$ 这一事实）

因此如果定理中所说的两个不等式都不成立的话，则必有

$$\left|\theta-\frac{p_{n-1}}{q_{n-1}}\right|\geqslant\frac{1}{2q_{n-1}^2} + \left|\theta-\frac{p_n}{q_n}\right|\geqslant\frac{1}{2q_n^2}$$

将这两个不等式相加就得出

$$\left|\theta-\frac{p_{n-1}}{q_{n-1}}\right|+\left|\theta-\frac{p_n}{q_n}\right|\geqslant\frac{1}{2q_n^2}+\frac{1}{2q_{n-1}^2}$$

而这与上面已证明的相反的不等式矛盾。所得的矛盾便说明定理中所说的两个不等式之中至少有一个成立。

引理 7.10 设 θ 是一个实数，$\frac{p_n}{q_n}$ 是 θ 的第 n 阶渐近分数，那么

(1) $q_n\theta-p_n$ 的符号和 $q_{n+1}\theta-p_{n+1}$ 的符号相反；

(2) $q_{n+1}p_n-q_np_{n+1}$ 的符号和 $q_n\theta-p_n$ 的符号相反；

(3) $q_n\mid q_{n+1}\theta-p_{n+1}\mid+q_{n+1}\mid q_n\theta-p_n\mid=1$。

证明 (1) 由引理 7.5 可知，θ 总是夹在两个相邻的渐近分数之间，也就是说，如果$\frac{p_n}{q_n}$和$\frac{p_{n+1}}{q_{n+1}}$是两个相邻的渐近分数，则其中必有一个比 θ 大，而另一个一定比 θ 小。因此

$$\left(\theta-\frac{p_n}{q_n}\right)\left(\theta-\frac{p_{n+1}}{q_{n+1}}\right)<0$$

因而
$$(q_n\theta-p_n)(q_{n+1}\theta-p_{n+1})<0$$

这就说明 $q_n\theta-p_n$ 的符号和 $q_{n+1}\theta-p_{n+1}$ 的符号相反；

(2) 我们有恒等式

$$q_{n+1}p_n-q_np_{n+1}=q_n(q_{n+1}\theta-p_{n+1})-q_{n+1}(q_n\theta-p_n)$$

因此如果 $q_n\theta-p_n<0$，那么由(1)已证明的结论可知

$$q_{n+1}\theta-p_{n+1}>0$$

因此由上面的恒等式得出

$$q_{n+1}p_n - q_n p_{n+1} > 0$$

同理可证如果 $q_n\theta - p_n > 0$,那么

$$q_{n+1}p_n - q_n p_{n+1} < 0$$

这就证明了(2)。

(3) 由(1)(2)可知,如果 $q_n\theta - p_n < 0$,那么 $q_{n+1}\theta - p_{n+1} > 0, q_{n+1}p_n - q_n p_{n+1} = 1$,因此这时

$$q_n \mid q_{n+1}\theta - p_{n+1} \mid + q_{n+1} \mid q_n\theta - p_n \mid =$$

$$q_n(q_{n+1}\theta - p_{n+1}) - q_{n+1}(q_n\theta - p_n) = q_{n+1}p_n - q_n p_{n+1} = 1$$

同理可证当 $q_n\theta - p_n > 0$ 时

$$q_n \mid q_{n+1}\theta - p_{n+1} \mid + q_{n+1} \mid q_n\theta - p_n \mid = 1$$

现在我们可以得出一个比定理 7.5 更好的结果。

定理 7.6 如果 θ 存在第 $n > 1$ 阶的渐近分数,则下面三个不等式

$$\left|\theta - \frac{p_{n-2}}{q_{n-2}}\right| < \frac{1}{\sqrt{5}q_{n-2}^2}, \left|\theta - \frac{p_{n-1}}{q_{n-1}}\right| < \frac{1}{\sqrt{5}q_{n-1}^2}, \left|\theta - \frac{p_n}{q_n}\right| < \frac{1}{\sqrt{5}q_n^2}$$

之中,至少有一个成立。

证明 设 $A_n = q_n \mid q_n\theta - p_n \mid$,那么由引理 7.10 可知

$$q_n \mid q_{n-1}\theta - p_{n-1} \mid + q_{n-1} \mid q_n\theta - p_n \mid = 1$$

$$\frac{q_n}{q_{n-1}}A_{n-1} + \frac{q_{n-1}}{q_n} = A_n = 1$$

因此,如果设 $\lambda = \frac{q_{n-1}}{q_n}$,则有 $\frac{1}{\lambda}A_{n-1} + \lambda A_n = 1$ 或 $\lambda^2 A_n - \lambda + A_{n-1} = 0$。

同理设 $\mu = \frac{q_{n+1}}{q_n}$,则有

$$\mu^2 A_n - \mu + A_{n+1} = 0$$

由 λ 和 μ 的定义可得

$$\mu - \lambda = \frac{q_{n+1} - q_{n-1}}{q_n} = \frac{a_n q_n + q_{n-1} - q_{n-1}}{q_n} = a_n$$

从 $\lambda^2 A_n - \lambda + A_{n-1} = 0$ 减去 $\mu^2 A_n - \mu + A_{n+1} = 0$ 并利用 $\mu - \lambda = a_n$ 就得到

$$a_n A_n(\lambda + \mu) = a_n + A_{n-1} - A_{n+1}$$

把上式平方再加上 $\mu - \lambda$ 的平方与 $a_n^2 A_n^2$ 的积得

$$2a_n^2 A_n^2(\lambda^2 + \mu^2) = a_n^4 A_n^2 + (a_n + A_{n-1} - A_{n+1})^2$$

用 $\lambda^2 A_n - \lambda + A_{n-1} = 0$ 加上 $\mu^2 A_n - \mu + A_{n+1} = 0$,有

$$A_n(\lambda^2 + \mu^2) - (\lambda + \mu) + (A_{n-1} + A_{n+1}) = 0$$

$$2a_n^2 A_n^2(\lambda^2 + \mu^2) - 2a_n^2 A_n(\lambda + \mu) + 2a_n^2 A_n(A_{n-1} + A_{n+1}) = 0$$

把 $2a_n^2A_n^2(\lambda^2+\mu^2)=a_n^4A_n^2+(a_n+A_{n-1}-A_{n+1})^2$ 和 $a_nA_n(\lambda+\mu)=a_n+A_{n-1}-A_{n+1}$ 代入上式得

$$a_n^4A_n^2+(a_n+A_{n-1}-A_{n+1})^2-2a_n(a_n+A_{n-1}-A_{n+1})+2a_n^2A_n(A_{n-1}+A_{n+1})=0$$

$$a_n^4A_n^2+2a_n^2A_n(A_{n-1}+A_{n+1})=2a_n(a_n+A_{n-1}-A_{n+1})-(a_n+A_{n-1}-A_{n+1})^2=$$
$$2a_n^2+2a_n(A_{n-1}-A_{n+1})-a_n^2-2a_n(A_{n-1}-A_{n+1})-(A_{n-1}-A_{n+1})^2=a_n^2-(A_{n-1}-A_{n+1})^2$$

因此 $(a_n^2+4)(\min(A_{n-1},A_n,A_{n+1}))^2\leqslant a_n^2A_n^2+2A_n(A_{n-1}+A_{n+1})\leqslant$

$$1-\frac{(A_{n-1}-A_{n+1})^2}{a_n^2}\leqslant 1$$

$$\min(A_{n-1},A_n,A_{n+1})\leqslant\sqrt{\frac{1}{a_n^2+4}}\leqslant\frac{1}{\sqrt{5}}$$

如果上面的不等式中出现等号,则 $a_n=1,A_k\geqslant\frac{1}{\sqrt{5}},k=n-1,n,n+1$ 并且

$$a_n^2A_n^2+2A_n(A_{n-1}+A_{n+1})=1$$

于是由 $a_n=1$ 得出

$$A_n^2+2A_n(A_{n-1}+A_{n+1})=1$$

$$\frac{2}{\sqrt{5}}\leqslant A_{n-1}+A_{n+1}=\frac{1-A_n^2}{2A_n}\leqslant\frac{1-(\frac{1}{\sqrt{5}})^2}{2}\sqrt{5}\leqslant\frac{2}{\sqrt{5}}$$

因此

$$A_{n-1}+A_{n+1}=\frac{2}{\sqrt{5}}$$

由于 A_{n-1},A_{n+1} 都是正数,因此如果 $A_{n-1}\neq A_{n+1}$,则它们之中必有一个数要小于$\frac{1}{\sqrt{5}}$,这与 $\min(A_{n-1},A_n,A_{n+1})=\frac{1}{\sqrt{5}}$ 矛盾,因此必须有

$$A_{n-1}=A_{n+1}=\frac{1}{\sqrt{5}}$$

再由 $A_n^2+2A_n(A_{n-1}+A_{n+1})=1$ 和 $A_n\geqslant\frac{1}{\sqrt{5}}$ 得出

$$a_n=1,A_{n-1}=A_n=A_{n+1}=\frac{1}{\sqrt{5}}$$

不难验证,$A_{n-1}=A_n=A_{n+1}$ 将导致0是一个有理数,这又导致 A_{n-1},A_n,A_{n+1} 这三个数都是有理数,而 $\min(A_{n-1},A_n,A_{n+1})=\frac{1}{\sqrt{5}}$ 又说明这三个数中的某一个数是一个无理数,这就得出矛盾,所得的矛盾说明必有

$$\min(A_{n-1},A_n,A_{n+1})<\frac{1}{\sqrt{5}}$$

设 k 表示 $n-1,n$ 或 $n+1$,则必有某一个 A_k 使得 $A_k<\frac{1}{\sqrt{5}}$ 或 $q_k\mid q_k\theta-p_k\mid<\frac{1}{\sqrt{5}}$,或 $\left|\theta-\frac{p_k}{q_k}\right|<\frac{1}{\sqrt{5}q_k^2}$,这就证明了定理。

定理 7.5 和定理 7.6 自然使人产生一种继续努力以得到更好的逼近常数的愿望,然而经过研究之后,发现常数 $\frac{1}{\sqrt{5}}$ 已不可能进一步改善,因此这一类型的定理就到此为止了。

事实上,如果我们考虑数 $\theta=\frac{\sqrt{5}+1}{2}=[1;1,1,\cdots]$,并设 $\frac{p_k}{q_k}$ 表示 θ 的第 k 阶渐近分数,r_k 表示它的第 k 阶余式的话,则易于看出对任何 k 都有 $r_k=\theta$。因此有

$$\theta=\frac{p_kr_{k+1}+p_{k-1}}{q_kr_{k+1}+q_{k-1}}=\frac{p_k\theta+p_{k-1}}{q_k\theta+q_{k-1}}$$

因而

$$\left|\theta-\frac{p_k}{q_k}\right|=\left|\frac{p_k\theta+p_{k-1}}{q_k\theta+q_{k-1}}-\frac{p_k}{q_k}\right|=\frac{1}{q_k(q_k\theta+q_{k-1})}=\frac{1}{q_k^2\left(\theta+\frac{q_{k-1}}{q_k}\right)}$$

但是由定理 6.1.1 得出 $\frac{q_k}{q_{k-1}}=[1;1,1,\cdots,1]$,因此当 $k\to\infty$ 时,$\frac{q_k}{q_{k-1}}\to\theta$。因而

$$\frac{q_{k-1}}{q_k}=\frac{1}{\theta}+\epsilon_k=\frac{\sqrt{5}-1}{2}+\epsilon_k$$

其中当 $k\to\infty$ 时,$\epsilon_k\to 0$。这样就得出

$$\left|\theta-\frac{p_k}{q_k}\right|=\frac{1}{q_k^2\left(\theta+\frac{q_{k-1}}{q_k}\right)}=\frac{1}{q_k^2\left(\frac{\sqrt{5}+1}{2}+\frac{\sqrt{5}-1}{2}+\epsilon_k\right)}=\frac{1}{q_k^2(\sqrt{5}+\epsilon_k)}$$

上面这个式子说明,对任何使得 $c<\frac{1}{\sqrt{5}}$ 的常数 c,当 k 充分大时,一定有

$$\left|\theta-\frac{p_k}{q_k}\right|>\frac{c}{q_k^2}$$

因而定理 7.6 中的常数 $\frac{1}{\sqrt{5}}$ 是不可能进一步改善的。

但是,这并不是说,对于某些特殊的无理数,逼近的程度也不可能再提高,事实上,如果我们限定考虑某些具有特别性质的无理数,就可能得到更好的逼近。

到现在为止,我们已经考虑了两类逼近问题,第一类逼近问题是问,任给实

数 θ 正数 $\epsilon > 0$，是否总存在整数 a,b 使得 $\left|\theta - \frac{a}{b}\right| < \epsilon$，第二类逼近问题是问任给实数 θ 正数 $\epsilon > 0$，是否总存在整数 a,b 使得 $|b\theta - a| < \epsilon$。由前面已经介绍的结果可知，这两类逼近问题都是有解的。

现在我们来考虑另一类所谓克罗内克逼近问题，即问任给了实数 θ 和 α 以及正数 $\epsilon > 0$，是否总存在整数 a,b 使得 $|b\theta - a - \alpha| < \epsilon$。然而当我们考虑这一类逼近问题时，我们发现，情况与以前所考虑过的两类逼近问题不同，出现了新的性质。这就是如果我们像以前那样允许实数 θ 和 α 是任意给定的话，问题将不再有解。

克罗内克(Kronecker, Leopold, 1823—1891)，德国数学家，生于利格尼茨，卒于柏林。

事实上，如果 $\theta = \frac{k}{h}$，$h > 0$ 是一个有理数的话，则设 $\alpha = \frac{1}{2h}$ 后，我们发现

$$|b\theta - a - \alpha| = \left|b\frac{k}{h} - a - \frac{1}{2h}\right| = \frac{|2(bk - ah) - 1|}{2h}$$

由于右边分数中的分子是一个奇数的绝对值，至少大于1，因此 $|b\theta - a - \alpha| \geqslant \frac{1}{2h}$，这说明量 $|b\theta - a - \alpha|$ 不可能变得任意小，因此我们遇到了一个无解的情况。为此，今后我们再考虑这种类型的逼近问题时，将总假设 θ 是无理的。在此条件下，不仅可使这类逼近问题总是有解，而且还可以发展出新的类型的逼近定理。

定理 7.7(切比雪夫)　对任意的无理数 θ 和实数 α，存在无穷多整数 a 和整数 $b > 0$，$b > 0$ 可以任意大，使得 $|b\theta - a - \alpha| < \frac{3}{b}$。

证明　设 $\frac{p}{q}$ 是无理数 θ 的任意渐近分数，则由定理 6.2.2 知 $\left|\theta - \frac{p}{q}\right| < \frac{1}{q^2}$，因此

$$\theta = \frac{p}{q} + \frac{\delta}{q^2}, 0 < |\delta| < 1$$

又对任意实数 α，设 t 是距离 $q\alpha$ 最近的整数，则必有 $|q\alpha - t| \leqslant \frac{1}{2}$，因此

$$\alpha = \frac{t}{q} + \frac{\delta'}{2q}, |\delta'| \leqslant 1$$

设 $\frac{r}{s}$ 是无理数 θ 的位于 $\frac{p}{q}$ 之前的与 $\frac{p}{q}$ 相邻的渐近分数，那么

$$qr - ps = \epsilon = \pm 1, q(\epsilon rt) - p(\epsilon st) = \epsilon^2 t = t$$

设 k 是一个任意整数，则从上式得出

$$p(kq - \epsilon st) - q(kp - \epsilon rt) = t$$

现在选取 k 使得 $\frac{q}{2} \leqslant kq - \epsilon st < \frac{3q}{2}$，并令 $kq - \epsilon st = b$，$kp - \epsilon rt = a$，那么显

然就有

$$\frac{q}{2} \leqslant b < \frac{3q}{2}, pb - qa = t$$

因此就有

$$|b\theta - a - \alpha| = \left|\frac{bp}{q} + \frac{b\delta}{q^2} - a - \frac{t}{q} - \frac{\delta'}{2q}\right| = \left|\frac{b\delta}{q^2} - \frac{\delta'}{2q}\right| < \frac{b}{q^2} + \frac{1}{2q}$$

因为 $q > \frac{2}{3}b$，所以

$$|b\theta - a - \alpha| < \frac{b}{q^2} + \frac{1}{2q} < \frac{9}{4b} + \frac{3}{4b} = \frac{3}{b}$$

而因为 θ 是无理数，所以 θ 存在分母为任意大的渐近分数，这也就是说，q 可以选得充分大，而由于 $b \geqslant \frac{q}{2}$，因此 b 也可以任意大。

由此定理显然立即可以推出克罗内克定理，即任给了无理数 θ 和实数 α 以及正数 $\epsilon > 0$，总存在整数 a, b 使得 $|b\theta - a - \alpha| < \epsilon$。然而这样做，就必须是用连分数的理论，因此我们以下给出一个单独的不依赖于连分数理论的证明。为此，我们首先证明一个其本身也很有兴趣的定理.

定理 7.8 设 θ 是一个无理数，那么叙列 $\{n\theta\}$ 在单位区间内是稠密的，即任给实数 α，$0 \leqslant \alpha \leqslant 1$，以及正数 $\epsilon > 0$，那么必存在正整数 n 使得

$$|\{n\theta\} - \alpha| < \epsilon$$

证明 首先注意，从 θ 是无理数得出如果 $m \neq n$，那么 $\{m\theta\} \neq \{n\theta\}$。其次由于 $n\theta = n[\theta] + n\{\theta\}$，我们得出

$$\{n\theta\} = \{n[\theta] + n\{\theta\}\} = \{n\{\theta\}\}$$

因而

$$|\{n\theta\} - \alpha| = |\{n\{\theta\}\} - \alpha|$$

现在 $\{\theta\}$ 已是一个适合 $0 < \{\theta\} < 1$ 的数了。所以我们只要对满足 $0 < \theta < 1$ 的无理数 θ 证明了定理，那么定理的结论就适合任意的无理数了。

设 $\epsilon > 0$ 并且已选好了任意一个实数 α，$0 \leqslant \alpha \leqslant 1$。那么对 $\epsilon > 0$，我们可选取正整数 N 使 $\frac{1}{N} < \epsilon$。由引理 7.2 对此 N 和实数 θ，必可选出整数对 $(h, k) = 1$，使得 $0 < k \leqslant N$，$|k\theta - h| < \frac{1}{N}$，令 $\beta = k\theta - h$，由于 θ 是无理数，故 $\beta \neq 0$，且 β 也是无理数。由于 $k\theta = h + \beta$，所以

$$mk\theta = mh + m\beta = mh - 1 + (1 + m\beta)$$

如果 $\beta > 0$，那么当且仅当 $0 < m\beta < 1$ 或者 $0 < \beta < \frac{1}{m}$ 时才有 $\{mk\theta\} = m\beta$。现在选取使得 $0 < \beta < \frac{1}{m}$ 成立的最大整数 M，那么我们就有

$$\{k\theta\} < \{2k\theta\} < \cdots < \{Mk\theta\}$$

其中 $M = \left[\frac{1}{\beta}\right] < \frac{1}{\beta}$。由于 β 是无理数以及由于 M 的最大性，我们就有

$$\frac{1}{M+1} < \beta < \frac{1}{M} \leqslant \frac{1}{N}$$

$$\frac{M}{M+1} < M\beta < 1$$

$$-1 < -M\beta < -\frac{M}{M+1}$$

$$0 < 1 - M\beta < 1 - \frac{M}{M+1} = \frac{1}{M+1} < \frac{1}{N}$$

因此 $\{k\theta\}, \{2k\theta\}, \cdots, \{Mk\theta\}$ 把 $[0,1]$ 区间分成了 $M+1$ 段，其中前 M 段的长度都是 β，最后一段的长度是 $1-M\beta$。因而从上面的不等式可知，这 $M+1$ 段中每一段的长度都小于 $\frac{1}{N}$。如果实数 $\alpha, 0 \leqslant \alpha \leqslant 1$，落到前 M 段的某一段中，则有

$$\{mk\theta\} \leqslant \alpha < \{(m+1)k\theta\}, 0 \leqslant m < M-1$$

$$0 \leqslant \alpha - \{mk\theta\} < \{(m+1)k\theta\} - \{mk\theta\} = \beta < \frac{1}{N}$$

如果 α 落到最后一段中则有

$$\{Mk\theta\} \leqslant \alpha \leqslant 1$$

$$0 \leqslant \alpha - \{Mk\theta\} \leqslant 1 - \{Mk\theta\} < \frac{1}{N}$$

因此无论发生哪种情况都存在一个正整数 $m > 0$ 使得

$$|\{mk\theta\} - \alpha| < \frac{1}{N} < \varepsilon$$

如果 $\beta < 0$，那么当且仅当 $0 < 1 + m\beta < 1$ 或者 $0 < -\beta < \frac{1}{m}$ 时才有 $\{mk\theta\} = 1 + m\beta$，那么选取使得 $0 < -\beta < \frac{1}{m}$ 成立的最大整数 M，那么我们就有

$$M = \left[-\frac{1}{\beta}\right] < -\frac{1}{\beta}, \frac{1}{M+1} < -\beta < \frac{1}{M} \leqslant \frac{1}{N}$$

$$1 + M\beta < 1 + (M-1)\beta < \cdots < 1 + \beta$$

或者

$$\{Mk\theta\} < \{(M-1)k\theta\} < \cdots < \{k\theta\}$$

$$\frac{M}{M+1} < -M\beta < 1$$

$$-1 < M\beta < -\frac{M}{M+1}$$

$$0 < 1 + M\beta < 1 - \frac{M}{M+1} \leqslant \frac{1}{M+1} < \frac{1}{N}$$

也就是 $1+M\beta, 1+(M-1)\beta, \cdots, 1+\beta$ 这 M 个点把 $[0,1]$ 区间分成了 $M+1$ 段，

其中后 M 段的长度都是 $-\beta$，第一段的长度是 $1+M\beta$。因而从上面的不等式可知，这 $M+1$ 段中每一段的长度都小于 $\frac{1}{N}$。与前面类似可证，无论实数 α 落到哪一段中都存在一个正整数 $m>0$ 使得

$$|\{mk\theta\}-\alpha|<\frac{1}{N}<\varepsilon$$

综合上面 $\beta>0$ 和 $\beta<0$ 两种情况的讨论就得到对任意实数 $\alpha, 0\leqslant\alpha<1$，正数 $\varepsilon>0$ 都存在一个正整数 $n=mk>0$，使得 $|\{n\theta\}-\alpha|<\varepsilon$。这就证明了定理。

引理 7.11 设 θ 是一个无理数，则任给实数 $\alpha, 0\leqslant\alpha\leqslant1$，以及正数 $\varepsilon>0$，必存在整数 $a, b, b>0$ 使得 $|b\theta-a-\alpha|<\varepsilon$。

证明 由定理 7.8 知，存在正整数 $b>0$ 使得 $|\{b\theta\}-\alpha|<\varepsilon$。令 $a=[b\theta]$，则

$$|b\theta-a-\alpha|=|b\theta-[b\theta]-\alpha|=|\{b\theta\}-\alpha|<\varepsilon$$

定理 7.9(克罗内克) 设 θ 是一个无理数，则任给实数 α 以及正数 $\varepsilon>0$，必存在整数 $a, b, b>0$ 使得 $|b\theta-a-\alpha|<\varepsilon$。

证明 令 $\alpha=[\alpha]+\{\alpha\}$，那么由定理 7.8 知存在正整数 $b>0$ 使得 $|\{b\theta\}-\{\alpha\}|<\varepsilon$。因此

$$|b\theta-[b\theta]-(\alpha-[\alpha])|<\varepsilon$$
$$|b\theta-([b\theta]-[\alpha])-\alpha|<\varepsilon$$

令 $a=[b\theta]-[\alpha]$，则 $|b\theta-a-\alpha|<\varepsilon$，这就证明了定理。

克罗内克逼近的进一步发展就是同时对多个线性型进行逼近，由此可以得出许多有力的结果，但是我们对这一问题的讨论就到此为止了，有兴趣的读者可以参考 TomM. Apostol 著《Modular Functions and Dirichlet Series in Number Theory》和朱尧辰，王联祥的《丢番图逼近引论》等书。

丢番图(Diophantus of Alexandria，活动于 250 ~ 275 前后)，希腊数学家，生平不详.

柳维尔(Liouville, Joseph, 1809—1882)，法国数学家. 生于加来海峡省圣奥梅尔，卒于巴黎.

现在我们来讲本节的最后一个逼近问题，即所谓的柳维尔逼近。

定理 7.10(柳维尔) 设 θ 是任意 $n(n>1)$ 次代数数，则必存在正数 $C>0$，使得对于任意整数 $a, b, b>0$ 都成立 $\left|\theta-\frac{a}{b}\right|>\frac{C}{b^n}$。

证明 首先注意，因为任何有理数都只能是一次代数数，所以在定理的条件下 θ 必是一个无理数。

设 θ 是整系数多项式 $f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n$ 的根，则

$$f(x)=(x-\theta)f_1(x)$$

如果 $f_1(\theta)=0$，则

$$f(x)=(x-\theta)^2f_2(x)$$

因此 $$f'(x)=2(x-\theta)f_2(x)+(x-\theta)^2f'_2(x)$$

从而 $f'(\theta)=0$，但 $f'(x)$ 是 $n-1$ 次的整系数多项式，这说明 θ 是 $n-1$ 次代数数，而这与假设矛盾，因此必有 $f_1(\theta)\neq 0$。

于是根据 $f_1(x)$ 的连续性可知必存在正数 $\delta>0$，使得当 $\theta-\delta\leqslant x\leqslant\theta+\delta$ 时 $f_1(x)\neq 0$。

设 $a,b,,b>0$ 是任意整数。如果 $\left|\theta-\frac{a}{b}\right|\leqslant\delta$，则根据 δ 的定义就有 $f_1\left(\frac{a}{b}\right)$。因此

$$\frac{a}{b}-\theta=\frac{f\left(\frac{a}{b}\right)}{f_1\left(\frac{a}{b}\right)}=\frac{a_0\left(\frac{a}{b}\right)^n+a_1\left(\frac{a}{b}\right)^{n-1}+\cdots+a_n}{f_1\left(\frac{a}{b}\right)}=$$

$$\frac{a_0a^n+a_1a^{n-1}b+\cdots+a_nb^n}{b^nf_1\left(\frac{a}{b}\right)}$$

最后所得的分数的分子是一个整数，且不等于0，因为否则就将有 $\frac{a}{b}-\theta=0$，因而将得出 $\theta=\frac{a}{b}$ 是一个有理数，但是我们一开始就说明了在定理的条件下 θ 只能是一个无理数。因此

$$|a_0a^n+a_1a^{n-1}b+\cdots+a_nb^n|\geqslant 1$$

设 M 表示连续函数 $f_1(x)$ 在闭区间 $[\theta-\delta,\theta+\delta]$ 上的上界，则

$$\left|\theta-\frac{a}{b}\right|=\left|\frac{a_0a^n+a_1a^{n-1}b+\cdots+a_nb^n}{b^nf_1\left(\frac{a}{b}\right)}\right|\geqslant$$

$$\frac{|a_0a^n+a_1a^{n-1}b+\cdots+a_nb^n|}{b^nM}\geqslant\frac{1}{b^nM}$$

如果 $\left|\theta-\frac{a}{b}\right|>\delta$，则 $\left|\theta-\frac{a}{b}\right|>\delta>\frac{\delta}{b^n}$。

令 $C=\min\left(\frac{1}{M},\delta\right)$，则综合上面两种情况的讨论就得到对任意整数 a,b，$b>0$ 都成立 $\left|\theta-\frac{a}{b}\right|>\frac{C}{b^n}$。这就证明了定理。

柳维尔定理的意义在于给出了一个代数数在逼近问题上的特性，因而也就同时给出了超越数在逼近问题上的特性。这个特性就是 $n(n>1)$ 次代数数不可能存在高于 n 阶的逼近。因而如果一个数能够具有高于任何 n 阶的逼近的话，这个数就必定是超越数。尽管在集合论中我们已预先知道了超越数的存在性。但那里并没有指出任何辨别一个具体的数究竟是否是超越数的方法，而柳维尔定理则指出了一个辨别的方法。这就是

定理 7.11 如果对于任意的常数 $C>0$ 和任意自然数 n,都存在满足不等式

$$\left|\theta-\frac{a}{b}\right|\leqslant\frac{C}{b^n}$$

的整数 a 和 b,$b>0$,则 θ 必是一个超越数。

上面在证明柳维尔定理时,我们假定了 $n>1$,并由此一直利用了 θ 是无理数的性质。实际上,柳维尔定理对有理数,即 $n=1$ 的情况也成立,由此我们可以得出一些辨别 θ 是有理数还是无理数的判据。

定理 7.12 如果 r 是一个有理数,则对任意使得 $\frac{a}{b}\neq r$ 的整数 a 和 b,$b>0$,存在与 a,b 无关的正常数 $C>0$,使得 $\left|r-\frac{a}{b}\right|\geqslant\frac{C}{b}$。

证明 设 $r=\frac{h}{k}$,$(h,k)=1$,$k>0$,则 k 与 a,b 无关而仅依赖于 r。于是

$$\left|r-\frac{a}{b}\right|=\left|\frac{h}{k}-\frac{a}{b}\right|=\frac{|bh-ak|}{bk}\geqslant\frac{1}{bk}$$

(上式中所得的分数的分子是一个整数且不为 0,否则将得出 $r=\frac{a}{b}$,与假设矛盾,由此即可得出最后的不等式)令 $C=\frac{1}{k}$ 就证明了定理。

定理 7.13 如果对实数 θ,存在整数 a_n,b_n,$b_n\to+\infty$ 和 $\delta>0$,使得不等式

$$0<\left|\theta-\frac{a_n}{b_n}\right|<\frac{M}{b_n^{1+\delta}}$$

成立(其中 M 是一个常数),则 θ 是无理数。

证明 假设 θ 是有理数,则由定理 7.12 知存在与 a_n,b_n 无关的正常数 C,使得

$$\frac{C}{q_n}\leqslant\left|\theta-\frac{a_n}{b_n}\right|<\frac{M}{q_n^{1+\delta}}$$

于是

$$q_n^{\delta}<\frac{M}{C}$$

由于 $\delta>0$,$q_n\to+\infty$,所以 $q_n^{\delta}\to+\infty$。这与上式矛盾,所得的矛盾便说明 θ 是无理数。

定理 7.14 设 θ 是一个实数,如果存在整数 a_n,b_n,$b_n\to+\infty$ 使得

$$|b_n\theta-a_n|>0,\ |b_n\theta-a_n|\to 0$$

则 θ 是无理数。

证明 设 $\varepsilon_n=|b_n\theta-a_n|$,如果 θ 是有理数,则由定理 7.12 知存在与 a_n,b_n 无关的正常数 C,使得

$$\left|\theta-\frac{a_n}{b_n}\right|\geqslant\frac{C}{b_n}$$

两边同乘以 $b_n>0$,不等式不变号。因此 $\varepsilon_n\geqslant C>0$,这与 $\varepsilon_n\to 0$ 矛盾,所得的矛盾便证明了 θ 是无理数。

例 7.1 证明:$\theta=\sum\limits_{n=1}^{\infty}\frac{1}{2^{n!}}=\frac{1}{2}+\frac{1}{4}+\frac{1}{64}+\cdots$ 是一个超越数。

证明 令 $a_n=2^{n!}\sum\limits_{i=1}^{n}\frac{1}{2^i}$, $b_n=2^{n!}$,则对任意常数 $C>0$,有

$$0<\theta-\frac{a_n}{b_n}=\sum_{i=n+1}^{\infty}\frac{1}{2^i}<\frac{1}{2^{(n+1)!}}\left(1+\frac{1}{2}+\frac{1}{2^2}+\cdots\right)\leqslant\frac{2}{2^{(n+1)!}}\leqslant\frac{C}{b_n^n}$$

因此根据定理 7.11 可知 θ 是一个超越数。

习题 7

1. (1) 设无限简单连分数 $\alpha=[a_0;a_1,a_2,\cdots]$ 的所有元素都有上界 $1\leqslant a_k\leqslant M$, $k=0,1,2,\cdots$, $\frac{p_k}{q_k}$ 是 α 的渐近分数,则 $\left|\alpha-\frac{p_k}{q_k}\right|>\frac{1}{(M+2)q_k^2}$。

(2) 设无限简单连分数 $\alpha=[a_0;a_1,a_2,\cdots]$ 的所有元素都有上界,则当 $c>0$ 充分小时,不等式 $\left|\alpha-\frac{p}{q}\right|<\frac{c}{q^2}$ 没有整数解 $p,q,q>0$。

(3) 如果无限简单连分数 $\alpha=[a_0;a_1,a_2,\cdots]$ 的元素没有上界,则对任意 $c>0$,不等式 $\left|\alpha-\frac{p}{q}\right|<\frac{c}{q^2}$ 有无穷多组整数解 $p,q,q>0$。

2. 证明:对任何整数 $p,q,q>0$, $\left|\sqrt{2}-\frac{p}{q}\right|>\frac{1}{3q^2}$。

3. 设实数 θ 的简单连分数展开式中所有的元素都大于或等于 2,证明:如果 θ 存在第 $n>1$ 阶的渐近分数,则下面三个不等式

$$\left|\theta-\frac{p_{n-2}}{q_{n-2}}\right|<\frac{1}{\sqrt{8}q_{n-2}^2},\quad\left|\theta-\frac{p_{n-1}}{q_{n-1}}\right|<\frac{1}{\sqrt{8}q_{n-1}^2},\quad\left|\theta-\frac{p_n}{q_n}\right|<\frac{1}{\sqrt{8}q_n^2}$$

之中,至少有一个成立。

实数的光谱:小数部分的性质

第八章

在物理中,各种谱,例如光谱,还有功率谱是认识物质性质的一种重要手段。你如果用镊子夹一点我们日常使用的食盐放在酒精喷灯或煤气喷灯上加热(一定要用喷灯,普通的酒精灯温度太低,观察不到这里所说的现象)。就会发现火焰会变成橘黄色,如果把这样发出的光通过分光镜就会得到由各种颜色组成的光条,这就是光谱。在这个光谱中会出现一条亮线,这就是食盐中钠原子受到激发后所发出的具有特定波长的谱线,把物质高温加热后,凡是光谱中出现了这条谱线的,则被检物质中必定含有钠原子,这一方法十分稳定和灵敏,不管你用食盐还是其他含钠的物质试验,都会检出这条谱线,而且只须要用极少的样品。所以物质的这一特性被发现以后,就迅速得到了应用,利用这一特性,科学家们研制成了光谱仪,用这种仪器,人们就可以迅速地知道太阳,乃至极为遥远的宇宙深处的星球是由什么物质组成的,也可以知道各种刑事案件中需要检验的物质的成分。现在这一方法已经形成了一种称为光谱分析的专门技术。

在物理中,还有一种谱叫做功率谱。利用这种谱,可以得知各种系统的状态。比如气象学家把气象变化的规律总结成所谓的微分方程,把这种微分方程经过简化可以得到一个由 3 个变量组成的叫做洛仑兹系统的方程。这个系统中含有 3 个参数,当你把参数调整到某些特定的值的时候,这个系统的功率谱就会

出现几条孤立的谱线，称为离散谱。这时系统中会出现周期解，表现在由这 3 个变量组成的相空间中可以观察到闭合的曲线。而当你把参数调整到另外一些特定的值的时候，这个系统的功率谱就会出现一片连在一起的谱线，看起来黑乎乎的，称为连续谱，这时系统处于所谓混沌状态，在相空间中可以观察到一种被称为"奇异吸引子"的东西，其形象就好像一团乱麻，系统的轨线（也就是微分方程的解曲线）在这团乱麻中可以任意地接近吸引子所在的空间中任意一点而又互不相交。不管是光谱还是功率谱，在物理学中都是认识物质及其运动的特性的重要手段。

在研究实数时，人们发现，对于实数，也可以绘制出类似于光谱的图像，这就是实数的小数部分。

任给一个实数 θ，把 $\{\theta\},\{2\theta\},\cdots,\{n\theta\},\cdots$ 标记在 $[0,1]$ 区间上，并在所得的每一点处，画一条垂直于数轴的有一定长度的线段，就可以得到一个类似于光谱的图像。对于不同的实数观察这一"光谱"，你会发现，有理数的"光谱"和无理数的"光谱"是很不一样的。简单地说，有理数的"光谱"都是离散谱，而无理数的"光谱"都是连续谱。当有理数的分母越来越大时，其"谱线"也越来越密，逐渐变的与连续谱用肉眼不可分辨。

8.1　小数部分的分布

首先看有理数的小数部分的分布。

显然有

引理 8.1.1　设 $r=\frac{p}{q},(p,q)=1,np=N(p)q+r_n,0\leqslant r_n<q$，则 $\{nr\}=\frac{r_n}{q}$。

由此可见，如果 r 是有理数，q 是 r 化成既约分数之后的分母，那么 $\{nr\}$ 只可能是 $0,\frac{1}{q},\frac{2}{q},\cdots,\frac{q-1}{q}$ 这 q 个点中的某一个。也就是说，我们有

引理 8.1.2　设 $r=\frac{p}{q},(p,q)=1,N_r=\{0,1,\{r\},\{2r\},\cdots,\{nr\},\cdots\}$，$Q_r=\{0,\frac{1}{q},\cdots,\frac{q-1}{q},1\}$，则 $N_r\subset Q_r$。

现在发生一个问题，就是虽然 $\{nr\}$ 只可能是 $0,\frac{1}{q},\frac{2}{q},\cdots,\frac{q-1}{q}$ 这 q 个点中的某一个。但是会不会不管取多少个 n，$0,\frac{1}{q},\frac{2}{q},\cdots,\frac{q-1}{q}$ 中总有些点取不到。通过试验，你会发现不会出现这种现象，而且如果出现这种现象，那这几个取不

到的点就有些怪了，很值得我们去深入地研究一下它们究竟有何特性才使得 $\{nr\}$ 取不到它们。不过事实上没有这种现象，然而这需要严格的证明。

定理 8.1.1　设 $r=\dfrac{p}{q}$，$(p,q)=1$，$N_r=\{0,1,\{r\},\{2r\},\cdots,\{nr\},\cdots\}$，$Q_r=\{0,\dfrac{1}{q},\cdots,\dfrac{q-1}{q},1\}$，则 $N_r=Q_r$。

证明　我们只须证明当 $m\neq n$，$0\leqslant m<q$，$0\leqslant n<q$ 时，$\{mr\}\neq\{nr\}$ 即可。

用反证法，假设 $\{mr\}=\{nr\}$，那么由引理 8.1.1 知 $r_m=r_n$。由于

$$mp\equiv r_m(\bmod q)$$

$$np\equiv r_m(\bmod q)$$

故

$$(m-n)p\equiv 0(\bmod q)$$

即

$$q\mid(m-n)p$$

但是由于 $(p,q)=1$，故 $q\mid(m-n)$。然而 $m\neq n$，$0\leqslant m<q$，$0\leqslant n<q$，因此 $|m-n|<q$，这与 $q\mid(m-n)$ 矛盾。所得的矛盾就证明了当 $m\neq n$，$0\leqslant m<q$，$0\leqslant n<q$ 时，$\{mr\}\neq\{nr\}$。

由以上证明可知 $\{r\},\{2r\},\cdots,\{qr\}$ 这 q 个点是两两不同的，而由引理 8.1.2 它们又只能取 $0,\dfrac{1}{q},\dfrac{2}{q},\cdots,\dfrac{q-1}{q}$ 这 q 个点，因此 $\{r\},\{2r\},\cdots,\{qr\}$ 就恰好是 $0,\dfrac{1}{q},\dfrac{2}{q},\cdots,\dfrac{q-1}{q}$ 这 q 个点的某种重新排列，这就证明了 $N_r=Q_r$。

当 n 继续增大时，$\{nr\}$ 将周期性地（周期为 q）重复，这就是有理数小数部分的分布。也就是说，如果 r 是有理数，那么 $\{nr\}$ 将只取有限个点，并且均匀地在这有限个点之间跳动。

但是如果 θ 是一个无理数，那么 $\{n\theta\}$ 的分布将和有理数大不一样，根据定理 7.8 我们有

定理 8.1.2　设 θ 是一个无理数，那么 $\{n\theta\}$ 在闭区间 $[0,1]$ 中稠密。

虽然我们已经知道对无理数 θ 来说 $\{n\theta\}$ 在闭区间 $[0,1]$ 中稠密，但是和有理数的情况一样，我们也会发生 $\{n\theta\}$ 是否会对闭区间 $[0,1]$ 中某些数特别"偏爱"的问题，尽管我们从直观上实在看不出有任何"偏爱"的理由，我们仍需对此给以严格的证明。为此我们首先给出无限多个点均匀分布的严格定义。

定义 8.1.1　设 ω 表示任一实数叙列 $\omega=\{x_1,x_2,\cdots,x_n,\cdots\}$，$n$ 是任意自然数，$E\subset[0,1]$ 是闭区间 $I=[0,1]$ 的任一子集，那么我们用 $N_n(E)$ 表示 $x_1,x_2,\cdots,x_n$ 中使得 $\{x_k\}\in E(1\leqslant k\leqslant n)$ 的项的个数（这里 $\{x_k\}$ 表示 x_k 的小数部分）。

定义 8.1.2　设 $\omega=\{x_1,x_2,\cdots,x_n,\cdots\}$，$I=[0,1]$，$E$ 是 I 的任意半开子区间 $[a,b)$，我们规定符号 E 既表示上面所说的子区间本身又表示这个子区间

的长度。那么如果

$$\lim_{n\to\infty}\frac{N_n(E)}{n}=E$$

则称点集 $\omega=\{x_1,x_2,\cdots,x_n,\cdots\}$ 在开区间(0,1)内一致分布(这里上式左边的 E 表示 I 的子区间,右边的 E 表示子区间的长度)。

假设 $\omega=\{x_1,x_2,\cdots,x_n,\cdots\}$ 在开区间(0,1)内一致分布,并设 $a\in I$ 是 I 中任意一个实数,取 E 是包含 a 且长度为充分小的半开子区间,那么由一致分布的定义就得出,对任意正数 $\epsilon>0$,存在无数多个 ω 中的数 x_{n_k},使得 $|\{x_{n_k}\}-a|<\epsilon$,这就是说,$\{x_n\}$ 在 I 中是稠密的。因此我们有

引理 8.1.3 $\omega=\{x_1,x_2,\cdots,x_n,\cdots\}$ 在开区间(0,1)内一致分布的必要条件是 (x_n) 在 I 中取到无穷多个点并且是稠密的。

由此引理立得

例 8.1.1 如果 r 是有理数,那么根据定理 8.1.1 就得出 $\{nr\}$ 在(0,1)中不可能是一致分布的。

所以一致分布虽然刻画了点分布的均匀性,但是这个概念只对无穷多个点有意义。

现在我们来证明一个无理数的另一个有别于有理数的特性,那就是如果 θ 是一个无理数,那么不仅 $\{n\theta\}$ 在(0,1)中是稠密的,而且还是一致分布的。

定理 8.1.3 设 θ 是一个无理数,那么 $\{n\theta\}$ 在(0,1)中是一致分布的。

证明 在证明之前,我们先来复习一下完全剩余系的概念。给定一个正整数 q,如果一个含有 q 个整数的集合 K 具有性质,K 中每个元素对于模 q 来说都是两两不同余的,则 K 就构成一个完全剩余系(见定义 3.11.2 和定理 3.11.1)。如果 K 是一个完全剩余系,那么 K 中元素除以 q 所得的余数就是集合 $\{0,1,2,\cdots,q-1\}$(定理 3.11.2)。

完全剩余系具有以下性质:

(1) 设 K 是完全剩余系,如果 $(a,q)=1$,那么 aK 也是完全剩余系(aK 表示用 a 去乘以 K 中每一个元素所得的集合)(定理 3.7.1);

(2) 设 K 是完全剩余系,b 是任意整数,那么 $K+b$ 也是完全剩余系($K+b$ 表示用 K 中每一个元素加上 b 所得的集合)(定理 3.7.2)。

完全剩余系这个概念特别适用于从总体上加以研究,比如设 $K=\{\xi_1,\xi_2,\cdots,\xi_q\}$ 构成一个模 q 的完全剩余系。如果你要问对 K 中一个特殊的元素 $\xi_i\left\{\frac{\xi_i}{q}\right\}$ 是什么,一般不好回答,但是如果要问 $\sum_{i=1}^{q}\left\{\frac{\xi_i}{q}\right\}$ 是多少,却很容易回答。因为根据完全剩余系的定义立即可知叙列 $\left\{\frac{\xi_1}{q}\right\},\left\{\frac{\xi_2}{q}\right\},\cdots,\left\{\frac{\xi_q}{q}\right\}$ 不过是叙列 $\frac{0}{q}$,

$\frac{1}{q},\cdots,\frac{q-1}{q}$ 的一个重新排列。

好了，现在我们就来证明定理 8.1。

设 $E=[a,b)$ 为 I 的任意半开子区间，$\frac{p_k}{q_k}$ 是 θ 的渐近分数，那么由定理 6.2.2 知

$$\left|\theta-\frac{p_k}{q_k}\right|<\frac{1}{q_kq_{k+1}}<\frac{1}{q_k^2},k\geqslant 0$$

因而存在无穷多对整数 $p,q(p,q)=1,q>0$ 可以任意大，使得

$$\left|\theta-\frac{p}{q}\right|<\frac{1}{q^2},(p,q)=1$$

因此 $$\theta-\frac{p}{q}=\frac{\delta}{q^2},\theta=\frac{p}{q}+\frac{\delta}{q^2},|\delta|<1$$

由于 q 可以任意大，因此存在 $M_1>0$，使当 $q>M_1$ 时有 $qb-qa=q(b-a)>2$，因而 (qa,qb) 中至少包含两个不相同的整数。于是我们可设

$u=\lceil qa\rceil$（qa 的天花板，即大于 qa 而又距离 qa 最近的整数）

$v=\lfloor qb\rfloor$（qb 的地板，即小于 ab 而又距离 qb 最近的整数）

并设 $u<v$，因此

$$u-1<qa\leqslant u<v\leqslant qb<v+1$$

$$\frac{u-1}{q}<a\leqslant\frac{u}{q}<\frac{v}{q}\leqslant b<\frac{v+1}{q}$$

再设 $n=hq+r,0\leqslant r<q$，于是任意一个 1 和 n 之间的整数 j 必可以写成

$$j=iq+k,0\leqslant i\leqslant h,0\leqslant k<q$$

的形式。这也就是说 $\{\theta\},\{2\theta\},\cdots,\{n\theta\}$ 这个数必被包含在下面的 $h+1$ 行，q 列的表中

$$\begin{matrix}0.\theta,0.\theta+1,\cdots,0.\theta+q-1\\1.\theta,1.\theta+1,\cdots,1.\theta+q-1\\\vdots\\h.\theta,h.\theta+1,\cdots,h.\theta+q-1\end{matrix}$$

对任意 $1\leqslant j\leqslant n$，我们又有

$$\{j\theta\}=\{(iq+k)\theta\}=\left\{(iq+k)\left(\frac{p}{q}+\frac{\delta}{q^2}\right)\right\}=$$

$$\left\{ip+\frac{kp}{q}+\frac{i\delta}{q}+\frac{k\delta}{q^2}\right\}=$$

$$\left\{\frac{kp}{q}+\frac{[i\delta]}{q}+\frac{\{i\delta\}+\frac{\delta k}{q}}{q}\right\}=$$

$$\left\{\frac{kp}{q}+\frac{[i\delta]}{q}+\frac{\delta''}{q}\right\}$$

其中 $\delta''=\{i\delta\}+\frac{\delta k}{q}$,因而

$$|\delta''|=\left|\{i\delta\}+\frac{\delta k}{q}\right|\leqslant\{i\delta\}+\left|\frac{\delta k}{q}\right|<1+\left|\frac{k}{q}\right|<2$$

由于$(p,q)=1$,$[i\delta]$与 q 无关,因此当 k 遍历$0,1,\cdots,q-1$这 q 个数时,$pk+[i\delta]$也遍历$0,1,\cdots,q-1$这 q 个数。这也就是说$\frac{kp}{q}+\frac{[i\delta]}{q}+\frac{\delta''}{q}$不过是$\frac{\delta''}{q},\frac{1}{q}+\frac{\delta''}{q},\cdots,\frac{q-1}{q}+\frac{\delta''}{q}$的一个重新排列。因而$\{\theta\},\{2\theta\},\cdots,\{n\theta\}$这 n 个数必被包含在下面的 $h+1$ 行,q 列的表中

$$\left\{\frac{\delta''}{q}\right\},\left\{\frac{1}{q}+\frac{\delta''}{q}\right\},\left\{\frac{q-1}{q}+\frac{\delta''}{q}\right\}$$
$$\left\{\frac{\delta''}{q}\right\},\left\{\frac{1}{q}+\frac{\delta''}{q}\right\},\left\{\frac{q-1}{q}+\frac{\delta''}{q}\right\}$$
$$\vdots$$
$$\left\{\frac{\delta''}{q}\right\},\left\{\frac{1}{q}+\frac{\delta''}{q}\right\},\left\{\frac{q-1}{q}+\frac{\delta''}{q}\right\}$$

这个表的每一行都是相同的,$\{\theta\},\{2\theta\},\cdots,\{n\theta\}$这 n 个数在上面这个表中共出现n 次。

现在我们考虑所有使得$0\leqslant\frac{i}{q}+\frac{\delta''}{q}<1$的 i,对应于满足这种关系 i 的$\left\{\frac{i}{q}+\frac{\delta''}{q}\right\}$当然只是上表中所有元素的一部分,对这种 i,显然有

$$\left\{\frac{i}{q}+\frac{\delta''}{q}\right\}=\frac{i}{q}+\frac{\delta''}{q}$$

因而为使$\left\{\frac{i}{q}+\frac{\delta''}{q}\right\}\in(a,b)$,只要 $a<\frac{i}{q}+\frac{\delta''}{q}<b$ 即可。

而由于

$$a\leqslant\frac{u}{q}<\frac{v}{q}\leqslant b$$

因此又只要

$$\frac{u}{q}<\frac{i}{q}+\frac{\delta''}{q}<\frac{v}{q}$$

或
$$u-\delta''<i<v-\delta''$$
即可。

但是因为 $|\delta''|\leqslant 2$,所以又有

$$u-\delta''\leqslant u+2,v-2\leqslant v-\delta''$$

因此又只要 $u+2\leqslant i\leqslant v-2$ 即可。

这也就是说，上面那个表中每一行里至少有 $v-2-(u+2)=v-v-4$ 个整数 i 可使得对应的 $\left\{\frac{i}{q}+\frac{\delta''}{q}\right\}\in(a,b)$，因而整个表中至少有 $(h+1)(v-u-4)$ 个 $\left\{\frac{i}{q}+\frac{\delta''}{q}\right\}\in(a,b)$，这也就是说 $\{\theta\},\{2\theta\},\cdots,\{n\theta\}$ 这 n 个数中，至少有 $(h+1)(v-u-4)$ 个数落到 (a,b) 中。

又因为对任何 i 都有

$$\frac{i-2}{q}\leqslant\frac{i}{q}+\frac{\delta''}{q}\leqslant\frac{i+2}{q}$$

所以满足上式的整数 i 除以 q 后至多是 $\frac{-2}{q},\frac{-1}{q},0,\frac{1}{q},\cdots,\frac{q-1}{q},1,\frac{q+1}{q}$ 这些数，其中有两个数小于 0，两个数大于 1，由此可以看出，满足 $\frac{i-2}{q}\leqslant\frac{i}{q}+\frac{\delta''}{q}\leqslant\frac{i+2}{q}$ 的整数 i 比满足 $0\leqslant\frac{i}{q}+\frac{\delta''}{q}<1$ 的整数 i 多了 4 个，满足 $0\leqslant\frac{i}{q}+\frac{\delta''}{q}<1$ 并且又要使得 $\left\{\frac{i}{q}+\frac{\delta''}{q}\right\}\in(a,b)$ 的整数 i 必须使得 $a<\frac{i}{q}+\frac{\delta''}{q}<b$，或 $qa<i+\delta''<qb$ 或 $qa-\delta''<i<qb+\delta''$。

由于 $u-1-\delta''<qa-\delta''<i<qb-\delta''<v+1-\delta''$，所以满足 $0\leqslant\frac{i}{q}+\frac{\delta''}{q}<1$ 并且又要使得 $\left\{\frac{i}{q}+\frac{\delta''}{q}\right\}\in(a,b)$ 的整数 i 至多有 $v+1-\delta''-(u-1-\delta'')=v-u+2$ 个，而上面表中每行里使得 $\left\{\frac{i}{q}+\frac{\delta''}{q}\right\}\in(a,b)$ 的整数 i 至多有 $v-u+2+4=v-u+6$ 个。这也就是说 $\{\theta\},\{2\theta\},\cdots,\{n\theta\}$ 这 n 个数中，至多有 $(h+1)(v-u+6)$ 个数落到 (a,b) 中。

根据上面的论述我们就得出

$$(h+1)(v-u-4)\leqslant N_n(E)\leqslant(h+1)(v-u+6)$$

由

$$\frac{u-1}{q}<a\leqslant\frac{u}{q}<\frac{v}{q}\leqslant b<\frac{v+1}{q}$$

得出
$$b-a<\frac{v+1}{q}-\frac{u-1}{q}$$

或
$$(b-a)q<v-u+2$$

以及
$$\frac{v}{q}-\frac{u}{q}\leqslant b-a$$

或
$$v-u\leqslant(b-a)q$$

因此
$$(b-a)q-2<v-u\leqslant(b-a)q$$

由此得出

$$(h+1)(v-u-4) > h(v-u-4) \geqslant \left(\frac{n-r}{q}\right)(v-u-4) \geqslant$$

$$\frac{n}{q}(v-u) - \frac{4n}{q} - \frac{r}{q}(v-u-4) \geqslant$$

$$\frac{n}{q}(q(b-a)-2) - \frac{4n}{q} - (v-u-4) \geqslant$$

$$n(b-a) - \frac{6n}{q} - (v-u-4) \geqslant$$

$$n(b-a) - \frac{6n}{q} - (q(b-a)-4) \geqslant$$

另一方面又有

$$(h+1)(v-u+6) \leqslant \left(\frac{n}{q}+1\right)(v-u+6) \leqslant$$

$$\frac{n}{q}(v-u) + \frac{6n}{q} + v - u + 6 \leqslant$$

$$n(b-a) + \frac{6n}{q} + v - u + 6 \leqslant$$

$$n(b-a) + \frac{6n}{q} + q(b-a) + 6$$

因而

$$b-a-\frac{6}{q}-\frac{q(b-a)-4}{n} < \frac{N_n(E)}{n} < b-a+\frac{6}{q}+\frac{q(b-a)+6}{n}$$

对任意 $\epsilon > 0$,由于 q 可以任意大,因此存在 $M_2 > 0$,使当 $q > M_2$ 时,$\frac{6}{q} < \frac{\epsilon}{2}$。现在固定 q,那么存在 $M_3 > 0$,使当 $n > M_3$ 时有

$$\frac{q(b-a)-4}{n} < \frac{\epsilon}{2}, \frac{q(b-a)+6}{n} < \frac{\epsilon}{2}$$

因而在 $n > M_3$ 时就有

$$E - \epsilon = b - a - \epsilon < \frac{N_n(E)}{n} < b - a + \epsilon < E + \epsilon$$

这就证明了 $\lim\limits_{n\to\infty}\frac{N_n(E)}{n} = E$,即 $\{n\theta\}$ 是一致分布的。

下面我们介绍一致分布的判断条件。首先研究必要条件,为此设叙列 x_n 是一致分布的。

引理 8.1.4 设 $\chi_E(x)$ 表示 E 的特征函数,即当 $x \in E$ 时 $\chi_E(x) = 1$,当 $x \notin E$ 时,$\chi_E(x) = 0$,那么叙列 x_n 是一致分布的充分必要条件是

$$\lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n}\chi_E(\{x_i\}) = \int_0^1 \chi_E(x)\mathrm{d}x$$

证明 由 $\sum_{i=1}^{n}\chi_E(\{x_i\}) = N_n(E)$ 和 $\int_0^1\chi_E(x)\mathrm{d}x = b - a = E$ 可知

$$\lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n}\chi_E(\{x_i\}) = \int_0^1\chi_E(x)\mathrm{d}x$$

不过是

$$\lim_{n\to\infty}\frac{N_n(E)}{n} = E$$

的另一种写法而已，这就证明了引理。

引理8.1.5 设叙列 x_n 是一致分布的，c 是一个常数，$f(x) = c\chi_E(x)$，那么

$$\lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n}f(\{x_i\}) = \int_0^1 f(x)\mathrm{d}x$$

证明 由叙列 $\{x_n\}$ 是一致分布的和引理 8.1.4 得出

$$\lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n}\chi_E(\{x_i\}) = \int_0^1\chi_E(x)\mathrm{d}x$$

因此

$$\lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n}c\chi_E(\{x_i\}) = \int_0^1 c\chi_E(x)\mathrm{d}x$$

这就是

$$\lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n}f(\{x_i\}) = \int_0^1 f(x)\mathrm{d}x$$

引理 8.1.6 设叙列 x_n 是一致分布的，$f(x)$ 是 $I = [0,1]$ 上的阶梯函数，那么

$$\lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n}f(\{x_i\}) = \int_0^1 f(x)\mathrm{d}x$$

证明 因为 $f(x)$ 是 $I = [0,1]$ 上的阶梯函数，因此 $f(x) = \sum_{j=1}^{k}f_j(x)$，其中 $f_i(x) = c_i\chi_{E_i}(x)$，$E_i = [a_i, a_{i+1})$，$0 = a_0 < a_1 < \cdots < a_k = 1$。

由叙列 x_n 是一致分布的和引理 8.1.5 知对每一个 j，成立

$$\lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n}f_j(\{x_i\}) = \int_0^1 f_j(x)\mathrm{d}x$$

因此

$$\lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n}f(\{x_i\}) = \lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n}\sum_{j=1}^{k}f_j(\{x_i\}) = \sum_{j=1}^{k}\lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n}f_j(\{x_i\}) =$$
$$\sum_{j=1}^{k}\int_0^1 f_j(x)\mathrm{d}x = \int_0^1\sum_{j=1}^{k}f_j(x)\mathrm{d}x = \int_0^1 f(x)\mathrm{d}x$$

这就证明了引理。

有了以上必要条件，现在我们就可以给出一个判断叙列 $\{x_n\}$ 是否是一致分布的充分必要条件了。

定理8.1.4 设 $f(x)$ 是 I 上的任意黎曼可积函数，则叙列 x_n 是一致分布的充分必要条件是

$$\lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n}f(\{x_i\})=\int_0^1 f(x)\mathrm{d}x$$

证明　首先证明必要性。设叙列 x_n 是一致分布的。

由于 $f(x)$ 是 I 上的黎曼可积函数，因此按照定积分的定义，对于任意 $\varepsilon>0$，存在 $\delta>0$，使得当 $\max(E_i,i=1,2,\cdots,k)<\delta$ 时就有

$$s<\sigma<S,0<S-s<\varepsilon$$

这里 $E_i=[a_i,a_{i+1}),0=a_0<a_1<\cdots<a_k=1,\sigma=\sum_{i=0}^{k-1}f(\xi_i)E_i$，$\xi_i$ 是 E_i 中任意一点（注意 E_i 既表示区间 $[a_i,a_{i+1})$，也表示区间 E_i 的长度）。s 和 S 分别表示达布下和与达布上和。

$$s=\sum_{i=0}^{k}m_iE_i,S=\sum_{i=0}^{k}M_iE_i$$

其中，m_i 是 $f(x)$ 在区间 E_i 上的下确界，M_i 是 $f(x)$ 在区间 E_i 上的上确界。

因此就存在两个阶梯函数

$$f_1(x,\varepsilon)=\sum_{i=0}^{k}m_i\chi_{E_i}(x),f_2(x,\varepsilon)=\sum_{i=0}^{k}M_i\chi_{E_i}(x)$$

使得

$$f_1(x,\varepsilon)\leqslant f(x)\leqslant f_2(x,\varepsilon)$$

并且

$$\int_0^1(f_2(x,\varepsilon)-f_1(x,\varepsilon))\mathrm{d}x=\int_0^1 f_2(x,\varepsilon)\mathrm{d}x-\int_0^1 f_1(x,\varepsilon)\mathrm{d}x=S-s<\varepsilon$$

由引理 8.1.6 知对于 $f_1(x,\varepsilon)$ 和 $f_2(x,\varepsilon)$ 成立

$$\lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n}f_1(x_i,\varepsilon)=\int_0^1 f_1(x,\varepsilon)\mathrm{d}x,\lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n}f_2(x_i,\varepsilon)=\int_0^1 f_2(x,\varepsilon)\mathrm{d}x$$

故

$$\int_0^1 f(x)\mathrm{d}x-\varepsilon\leqslant\int_0^1 f_1(x)\mathrm{d}x\leqslant\lim_{n\to\infty}\frac{1}{n}\sum_{i=0}^{n}f_1(\{x_i\},\varepsilon)\leqslant$$

$$\underline{\lim_{n\to\infty}}\frac{1}{n}\sum_{i=0}^{n}f(\{x_i\})\leqslant\overline{\lim_{n\to\infty}}\frac{1}{n}\sum_{i=0}^{n}f(\{x_i\})\leqslant$$

$$\lim_{n\to\infty}\frac{1}{n}\sum_{i=0}^{n}f_2(\{x_i\},\varepsilon)\leqslant\int_0^1 f_2(x)\mathrm{d}x\leqslant\int_0^1 f(x)\mathrm{d}x+\varepsilon$$

由于当 n 充分大时

$$\underline{\lim_{n\to\infty}}\frac{1}{n}\sum_{i=0}^{n}f(\{x_i\})\leqslant\frac{1}{n}\sum_{i=0}^{n}f(\{x_i\})\leqslant\overline{\lim_{n\to\infty}}\frac{1}{n}\sum_{i=0}^{n}f(\{x_i\})$$

因而存在 $M>0$，使当 $n>M$ 时有

$$\int_0^1 f(x)\mathrm{d}x-\varepsilon\leqslant\frac{1}{n}\sum_{i=1}^{n}f(\{x_i\})\leqslant\int_0^1 f(x)\mathrm{d}x+\varepsilon$$

而由 ε 的任意性就说明当 $n\to\infty$ 时，极限 $\lim_{n\to\infty}\frac{1}{n}\sum_{i=0}^{n}f(\{x_i\})$ 存在，且

黎曼（Riemann, Georg Friedrich Bernhard, 1826—1866），德国数学家．生于德国丹嫩贝格附近，卒于意大利北部马焦雷湖畔．

$$\lim_{n\to\infty}\frac{1}{n}\sum_{i=0}^{n}f(\{x_i\})=\int_0^1 f(x)\mathrm{d}x$$

这就证明了必要性。

现在证明充分性。假设对一切 I 上的黎曼可积函数 $f(x)$ 都成立以上等式，则我们可取 $f(x)$ 为 E 的特征函数，于是根据引理 8.1.4 即得叙列 x_n 是一致分布的。

上面这个定理虽然给出了判断叙列 x_n 是否是一致分布的充分必要条件，但是实际运用起来十分困难，因为只有对 I 上的所有黎曼可积函数验证才能证明 x_n 的一致分布性。为此，我们还需得出更为实用的判别法。

引理 8.1.7　设 $f(x)$ 是实轴上任意周期为 1 的复值连续周期函数，则叙列 $\{x_n\}$ 是一致分布的充分必要条件是

$$\lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n}f(\{x_i\})=\int_0^1 f(x)\mathrm{d}x$$

证明　设 $E=[a,b)$ 是 $I=[0,1]$ 的任意子区间。

首先证明必要性。设叙列 x_n 是一致分布的，那么因为连续函数当然都是黎曼可积的，所以对 $f(x)$ 的实部和虚部分别应用定理 8.1.4，首先得出对每一个定义在实轴上的复值连续函数 $f(x)$ 成立

$$\lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n}f(\{x_i\})=\int_0^1 f(x)\mathrm{d}x$$

然而由 $f(x)$ 是周期为 1 的周期函数的假设可以得出 $f(\{x_n\})=f(x_n)$，这样就得出对每一个定义在实轴上的周期为 1 的复值连续周期函数 $f(x)$ 成立

$$\lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n}f(x_i)=\int_0^1 f(x)\mathrm{d}x$$

为证充分性，设对任意定义在实轴上的周期为 1 的复值连续周期函数 $f(x)$ 上式成立。

任给 $\varepsilon>0$，必存在两个定义在 I 上的连续函数 $g_1(x)$ 和 $g_2(x)$，使得

$$g_1(x)\leqslant\chi_E(x)\leqslant g_2(x)$$

并且

$$\int_0^1(g_2(x)-g_1(x))\mathrm{d}x\leqslant\varepsilon$$

现在把 $g_1(x)$ 和 $g_2(x)$ 周期都为 1 的延拓到整个数轴上，就得到两个定义在实轴上的周期为 1 的复值连续周期函数 $f_1(x)$ 和 $f_2(x)$，因而按照假设对它们成立

$$\lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n}f_1(x_i)=\int_0^1 f_1(x)\mathrm{d}x,\ \lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n}f_2(x_i)=\int_0^1 f_2(x)\mathrm{d}x$$

因此

$$E-\varepsilon\leqslant\int_0^1 g_2(x)\mathrm{d}x-\varepsilon\leqslant\int_0^1 g_1(x)\mathrm{d}x\leqslant$$

$$\int_0^1 f_1(x)\mathrm{d}x \leqslant \lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n} f_1(x_i) \leqslant$$

$$\underline{\lim}_{n\to\infty}\frac{N_n(E)}{n} \leqslant \overline{\lim}_{n\to\infty}\frac{N_n(E)}{n} \leqslant$$

$$\lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n} f_2(x_i) \leqslant \int_0^1 f_2(x)\mathrm{d}x \leqslant$$

$$\int_0^1 g_2(x)\mathrm{d}x \leqslant \int_0^1 g_1(x)\mathrm{d}x + \varepsilon \leqslant E + \varepsilon$$

由于当 n 充分大时

$$\underline{\lim}_{n\to\infty}\frac{N_n(E)}{n} \leqslant \frac{N_n(E)}{n} \leqslant \overline{\lim}_{n\to\infty}\frac{N_n(E)}{n}$$

因此就存在 $M > 0$，使当 $n > M$ 时，有

$$E - \varepsilon \leqslant \frac{N_n(E)}{n} \leqslant E + \varepsilon$$

这就证明了当 $n \to \infty$ 时，极限 $\lim\limits_{n\to\infty}\frac{N_n(E)}{n}$ 存在，且 $\lim\limits_{n\to\infty}\frac{N_n(E)}{n} = E$，于是根据定义就得出叙列 x_n 是一致分布的。

外尔（Weyl, Claude Hugo Hermann, 1885—1955），德国数学家，生于德国汉堡附近的埃尔姆斯霍恩.

定理 8.1.5（外尔判据） 设 h 是任意非零整数，则叙列 x_n 是一致分布的充分必要条件是

$$\lim_{n\to\infty}\frac{1}{n}\sum_{i=0}^{n} \mathrm{e}^{2\pi i h x_n} = 0$$

证明 先证必要性。设叙列 x_n 是一致分布的。考虑函数 $f(x) = \mathrm{e}^{2\pi i h x}$，这显然是一个定义在全数轴上的周期为 1 的连续周期函数，因此由引理 8.1.7 即得

$$\lim_{n\to\infty}\frac{1}{n}\sum_{k=1}^{n} \mathrm{e}^{2\pi i h x} = \int_0^1 \mathrm{e}^{2\pi i h x}\mathrm{d}x = \frac{1}{2\pi i h}\mathrm{e}^{2\pi i h x}\Big|_0^1 = 0$$

为证明充分性，假设对于叙列 x_n，$\lim\limits_{n\to\infty}\frac{1}{n}\sum\limits_{k=0}^{n}\mathrm{e}^{2\pi i h x_k} = 0$。我们证明对一切定义在全数轴上的周期为 1 的连续周期函数 $f(x)$ 成立

$$\lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n} f(x_i) = \int_0^1 f(x)\mathrm{d}x$$

设 $\varepsilon > 0$ 是任意正数，那么由维尔斯特拉斯逼近定理可知存在一个有有限多个带有复系数的形如 $\mathrm{e}^{2\pi i h x}$（这里，h 是一个整数）的项组成的三角多项式 $\psi(x)$（$\psi(x)$ 显然具有周期 1，因而是一个定义在全数轴上的周期为 1 的连续周期函数）使得

$$\sup_{0\leqslant x\leqslant 1} |f(x) - \psi(x)| \leqslant \frac{\varepsilon}{3}$$

（见：那汤松. 函数构造论（上册）. 上海：科学出版社，1958，5）。我们有

$$\left|\int_0^1 f(x)\mathrm{d}x - \frac{1}{n}\sum_{i=0}^{n} f(x_i)\right| \leqslant \left|\int_0^1 (f(x) - \psi(x))\mathrm{d}x\right| + \left|\int_0^1 \psi(x) - \frac{1}{n}\sum_{i=0}^{n}\psi(x_i)\right| + \left|\frac{1}{n}\sum_{i=0}^{n}(f(x_i) - \psi(x_i))\right|$$

上面不等式的右端中,由于$\sup\limits_{0\leqslant x\leqslant 1}|f(x) - \psi(x)| \leqslant \frac{\varepsilon}{3}$,因此第一项和第三项对任何 n 都是小于$\frac{\varepsilon}{3}$ 的,而由引理 8.1.7 可知,存在 $M > 0$,使当 $n > M$ 时

$$\left|\int_0^1 \psi(x) - \frac{1}{n}\sum_{i=0}^{n}\psi(x_i)\right| < \frac{\varepsilon}{3}$$

因而使当 $n > M$ 时

$$\left|\int_0^1 f(x)\mathrm{d}x - \frac{1}{n}\sum_{i=0}^{n} f(x_i)\right| < \frac{\varepsilon}{3} + \frac{\varepsilon}{3} + \frac{\varepsilon}{3} \leqslant \varepsilon$$

因此由 ε 的任意性就证明了对一切定义在全数轴上的周期为 1 的连续周期函数 $f(x)$ 成立

$$\lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n} f(x_i) = \int_0^1 f(x)\mathrm{d}x$$

根据引理引理 8.1.7 就得出叙列 x_n 是一致分布的,这就证明了充分性。由于

$$\left|\frac{1}{n}\sum_{k=0}^{n}\mathrm{e}^{2\pi\mathrm{i}h k\theta}\right| \leqslant \frac{1}{n}|\mathrm{e}^{\mathrm{i}\varphi} + \mathrm{e}^{2\mathrm{i}\varphi} + \cdots + \mathrm{e}^{\mathrm{i}n\varphi}|, \varphi = 2\pi h\theta \leqslant$$
$$\frac{1}{n}|\mathrm{e}^{\mathrm{i}\varphi}||1 + \mathrm{e}^{\mathrm{i}\varphi} + \cdots + \mathrm{e}^{\mathrm{i}(n-1)\varphi}| \leqslant \frac{|\mathrm{e}^{\mathrm{i}\varphi}||\mathrm{e}^{\mathrm{i}n\varphi} - 1|}{n|\mathrm{e}^{\mathrm{i}\varphi} - 1|} \leqslant$$
$$\frac{1}{n}\sqrt{\frac{(1 - \cos n\varphi)^2 + \sin^2 n\varphi}{(1 - \cos\varphi)^2 + \sin^2\varphi}} \leqslant$$
$$\frac{\left|\sin\frac{n\varphi}{2}\right|}{n\left|\sin\frac{\varphi}{2}\right|} \leqslant \frac{1}{n|\sin\pi h\theta|}$$

以及当 θ 是无理数时,对任何非零整数 h, $\sin\pi h\theta \neq 0$,因此当 $n\to\infty$ 时 $\frac{1}{n}\sum_{i=0}^{n}\mathrm{e}^{2\pi\mathrm{i}h\theta} \to 0$,故根据定理 8.1.5 就重新得出定理 8.1.3 这个证明比原来的证明就简短多了,不过别忘了,这是以一大堆准备工作为代价的,如果算上所有这些准备工作,整个证明也不见得比直接证明简短。不过,从这个例子也可看出,定理 8.1.5 的威力确实是很强大的,所以如果不单是为了得出定理 8.1.3,还是很有价值的。

习题 8.1

1. 设 a,b 都是整数 $r=\frac{a}{b},(a,b)=1,a>0,b>0,0<r<1$。把 $x_1=\{0r\},x_2=\{r\},\cdots,x_b=\{(b-1)r\}$ 这 b 个点按如下方式排成一个表 A：

首先在第一行写下 $x_1,x_2,\cdots,x_{n_1}$ 使得 $x_{n_1}<1,x_{n_1}+r>1$；然后在第二行写下 $x_{n_1+1}=x_{n_1}+r-1,x_{n_1+2}=x_{n_1+1}+r,\cdots,x_{n_2}$ 使得 $x_{n_2}<1,x_{n_2}+r>1$；在第三行写下 $x_{n_2+1}=x_{n_2}+r-1,x_{n_2+2}=x_{n_2+1}+r,\cdots,x_{n_3}$ 使得 $x_{n_3}<1,x_{n_3}+r>1\cdots$ 以下依此类推。

又设 $b=qa+r,0\leqslant r<a$。证明：

(1) A 的每一行至少有 q 个元素，至多有 $q+1$ 个元素；

(2) A 一共有 a 行；

(3) A 中有 r 行含有 $q+1$ 个元素，有 $a-r$ 行含有 q 个元素。

2. 设 $\theta=0.123\,456\,789\,101\,112\,131\,4\cdots$ 表示在小数点之后顺次写上所有的自然数所得的小数，证明：

(1) θ 是无理数，因此 $\{n\theta\}$ 在 $I=[0,1]$ 中是稠密的，一致分布的；

(2) $\{10^n\theta\}$ 在 $I=[0,1]$ 中也是稠密的。

3. 设 e 表示自然对数的底，证明：

(1) e 是无理数，因此 $\{n\mathrm{e}\}$ 在 $I=[0,1]$ 中是稠密的，一致分布的；

(2) $\{n!\mathrm{e}\}$ 在 $I=[0,1]$ 中不是稠密的。

4. 证明：如果 x_n 是一致分布的，α 是一个实常数，那么 $x_n+\alpha$ 也是一致分布的。

5. 设 x_n 是一致分布的，α 是一个实常数，y_n 使得 $\lim\limits_{n\to\infty}(x_n-y_n)=\alpha$，则 y_n 也是一致分布的。

6. 设 x_n,y_n 都是一致分布的，则叙列 $x_1,y_1,x_2,y_2,\cdots,x_n,y_n,\cdots$ 也是一致分布的。

7. 设 θ 是一个无理数，证明：叙列 $0,\theta,-\theta,2\theta,-2\theta,\cdots$ 是一致分布的。

8. 设 u,v 是两个任意实数，证明：$|\mathrm{e}^{2\pi iu}-\mathrm{e}^{2\pi iv}|\leqslant 2\pi|u-v|$。

9. 设 θ 是一个无理数，叙列 x_n 具有性质：当 $n\to\infty$ 时，$\Delta x_n=x_{n+1}-x_n\to\theta$，证明：

(1) 对每一个正整数 $q>0$，都存在一个正数 $M(q)>0$，使得对任意 $m>n>M(q)$ 都成立

$$|x_m-x_n-(m-n)\theta|<\frac{m-n}{q^2}$$

(2) $\left|\sum\limits_{j=n}^{m-1}(\Delta x_j-\theta)\right|=|x_m-x_n-(m-n)\theta|$；

(3) 设 h 是一个非零整数，则 $|e^{2\pi i h x_n} - e^{2\pi i h(x_n+(m-n)\theta)}| \leqslant \dfrac{2\pi|h|(m-n)}{q^2}$；

(4) $\left|\sum_{j=n}^{n+q-1} e^{2\pi i h x_j}\right| \leqslant \left|\sum_{j=n}^{n+q-1} e^{2\pi i h(x_n+(j-n)\theta)}\right| + \dfrac{2\pi|h|}{q^2}\sum_{j=n}^{n+q-1}(j-n) \leqslant K$，其中

$$K = \frac{1}{|\sin \pi h\theta|} + \frac{\pi}{|h|}$$

(5) 设 H 是一个正整数，则 $\left|\sum_{j=n}^{n-1+Hq} e^{2\pi i h x_j}\right| \leqslant HK$；

(6) $\left|\sum_{j=1}^{m} e^{2\pi i h x_j}\right| \leqslant n - 1 + \dfrac{m-n}{q}K + q$；

(7) 固定 q，则 $\overline{\lim_{m\to\infty}}\left|\dfrac{1}{m}\sum_{j=1}^{m} e^{2\pi i h x_j}\right| \leqslant \dfrac{K}{q}$；

(8) 令 q 充分大，证明：x_n 是一致分布的。

10. 设 x_n 是一个实数叙列，$E = [a,b)$ 是 $I = [0,1]$ 的任意子区间，$N_E(k,h)$ 表示 $\{x_{k+1}\},\{x_{k+2}\},\cdots,\{x_{k+h}\}$ 这些项里落入到 E 中的数目，如果对 $k = 0,1,2,\cdots$ 一致地成立

$$\lim_{n\to\infty}\frac{N_E(k,h)}{n} = E$$

则称 x_n 是良分布的，证明良分布的序列一定是一致分布的。

11. 设 x_n 是一致分布的序列，$m = 1,2,\cdots$ 是自然数，令 $y_n = 0$，如果 $m^3 + 1 \leqslant n \leqslant m^3 + m$；对其他的 n，则令 $y_n = x_n$。证明：

(1) $|N_E(n,x_n) - N_E(n,y_n)| \leqslant n^{\frac{2}{3}}$；

(2) 叙列 y_n 也是一致分布的；

(3) 叙列 y_n 不可能是良分布的。

12. 设叙列 x_n 是良分布的，$E = [a,b)$ 是 $I = [0,1]$ 的任意子区间，则一定存在一个整数 Q 使得 x_n 的任意接连的 Q 项中，至少有一项落入 E 中。

13. 设叙列 x_n 具有性质当 $n\to\infty$ 时，$\Delta x_n = x_{n+1} - x_n \to 0$，证明：$x_n$ 不可能是良分布的。

14. 证明：$\lg n$ 不可能是良分布的。

15. 证明：$\lg n$ 不是一致分布的。(提示：利用第 3 章定理 3.8.5(2) 中的欧拉求和公式

$$\sum_{k=1}^{n} f(k) = \int_1^n f(x)\mathrm{d}x + \frac{1}{2}(f(n) + f(1)) + \int_1^n B_1(\{x\})f'(x)\mathrm{d}x)$$

8.2 殊途同归——有理数和无理数小数部分的一个共同性质

我们在前面已经介绍了有理数和无理数的许多不一样的性格，例如它们的小数表示和连分数表示的不同，它们的逼近性质的差异，它们的小数部分在稠密性和一致分布方面的鲜明反差。因此有理数和无理数看起来是如此不同，尤其是在小数部分方面，以致很难想象他们在此方面还能有什么共同点。但是事情就是这么奇怪，有理数和无理数的小数部分的分布居然也会造成一个同样的现象，就是不管 θ 是有理数还是无理数，$\{\theta\},\{2\theta\},\cdots,\{n\theta\}$ 这 n 个点把区间 $(0,1)$ 分成的 $n+1$ 个小区间的长度最多只能取 3 个值，而且当这些区间的长度取到 3 个值时，其中最大的值必等于另外两个值之和。虽然这初听起来有些不可思议，但实践是检验真理的唯一标准，面对事实，你只能承认并加以研究。

引理 8.2.1 设 θ 是无理数，因而 $\{n\theta\}+\{\theta\}\neq 1$，则如果 $\{n\theta\}+\{\theta\}<1$，那么 $\{(n+1)\theta\}=\{n\theta\}+\{\theta\}$，如果 $\{n\theta\}+\{\theta\}>1$，那么 $\{(n+1)\theta\}=\{n\theta\}+\{\theta\}-1$。

证明 如果 $\{n\theta\}+\{\theta\}<1$，那么

$$(n+1)\theta=n\theta+\theta=[n\theta]+[\theta]+\{n\theta\}+\{\theta\}$$

因此

$$\{(n+1)\theta\}=\{n\theta\}+\{\theta\}$$

如果 $\{n\theta\}+\{\theta\}>1$，那么

$$1<\{n\theta\}+\{\theta\}<2$$

$$0<\{n\theta\}+\{\theta\}-1<1$$

$$(n+1)\theta=n\theta+\theta=[n\theta]+[\theta]+\{n\theta\}+\{\theta\}=$$
$$[n\theta]+[\theta]+1+\{n\theta\}+\{\theta\}-1$$

因此

$$\{(n+1)\theta\}=\{n\theta\}+\{\theta\}-1$$

引理 8.2.2 设 θ 是无理数，如果 $\{n\theta\}<\{k\theta\}$，$\{(n+1)\theta\}=\{n\theta\}+\{\theta\}-1$，那么

$$\{(n+1)\theta\}<\{(k+1)\theta\}<\{k\theta\}$$

证明 由 $\{(n+1)\theta\}=\{n\theta\}+\{\theta\}-1$ 得出 $\{n\theta\}+\{\theta\}>1$，因而

$$\{k\theta\}+\{\theta\}>\{n\theta\}+\{\theta\}>1$$

故由引理 8.2.1 得出

$$\{(k+1)\theta\}=\{k\theta\}+\{\theta\}-1<\{k\theta\}$$

$$\{(n+1)\theta\}\leqslant\{n\theta\}+\{\theta\}-1<\{k\theta\}+\{\theta\}-1\leqslant\{(k+1)\theta\}<\{k\theta\}$$

引理 8.2.3 设 θ 是一个实数，把 $x_0=\{0\theta\},x_1=\{\theta\},\cdots,x_n=\{n\theta\}$ 按

如下方式在 $I=[0,1]$ 中轮流写下以下各数：

在第一轮写下 $x_0,x_1\cdots,x_{n_1}$，使得 $x_{n_1}<1,x_{n_1}+\{\theta\}>1$；

在第二轮写下 $x_{n_1+1}=x_{n_1}+\{\theta\}-1,x_{n_1+2}=x_{n_1+1}+\{\theta\},\cdots,x_{n_2}$，使得 $x_{n_2}<1,x_{n_2}+\{\theta\}>1$；

在第三轮写下 $x_{n_2+1}=x_{n_2}+\{\theta\}-1,x_{n_2+2}=x_{n_1+1}+\{\theta\},\cdots,x_{n_3}$，使得 $x_{n_3}<1,x_{n_3}+\{\theta\}>1$；

…

以后依次类推。

求证：第 k 轮的点具有表达式 $x_n=n\{\theta\}-k+1$。

证明　第一轮的点具有特点

$$x_n=\{n\theta\}=n\{\theta\}=n\{\theta\}-1+1$$

因此引理对于自然数 $k=1$ 成立。

假设引理对于自然数 k 成立，即假设第 k 轮的点具有表达式

$$(n_{k-1}+1)\{\theta\}-k+1,(n_{k-1}+2)\{\theta\}-k+1,\cdots,n_k(\theta)-k+1$$

那么按照引理中解数的规则，第 $k+1$ 轮中的点就应该具有表达式

$$\begin{aligned}x_{n_k+1}&=x_{n_k}+\{\theta\}-1=n_k\{\theta\}-k+1+\{\theta\}-1=\\&(n_k+1)\{\theta\}-k=(n_k+1)\{\theta\}-(k+1)+1\\x_{n_k+2}&=x_{n_k+1}+\{\theta\}=(n_k+1)\{\theta\}-k+\{\theta\}=\\&(n_k+2)\{\theta\}-k=(n_k+2)\{\theta\}-(k+1)+1\\&\vdots\\x_{n_{k+1}}&=x_{n_{k+1}-1}+\{\theta\}=(n_{k+1}-1)\{\theta\}-k+\{\theta\}=\\&n_{k+1}\{\theta\}-k=n_{k+1}\{\theta\}-(k+1)+1\end{aligned}$$

这就说明引理对自然数 $k+1$ 也成立，因此由数学归纳法就证明了引理。

引理 8.2.4　设 θ 是一个实数，$x_n=\{n\theta\}$。x_{k-1},x_k 是第 $s+1$ 轮的两个相邻的点，那么区间 (x_{k-1},x_k) 之中必包含且仅包含 s 个分点 $x_{i_1},x_{i_2},\cdots,x_{i_s}$ 使得分点 x_{i_j} 是第 $j(j<s+1)$ 轮的，因此 $i_j<k-1$。

证明　按照我们写数的规定，在每一轮中，相邻两个数之间的距离都是 $d=\{\theta\}$，因此在每一轮中，区间 $I=[0,1]$ 都被这一轮的点（不包括其他轮的点）划分为一些至多长 d 的小区间，且由于分点是两两不同的，因此 x_{k-1} 和 x_k 不可能与前 s 轮中的任何一个分点重合。因此长为 d 的区间 (x_{k-1},x_k) 必包含且仅包含前 s 轮中的一个点 x_{i_j} 使得分点 x_{i_j} 是第 j 轮的，$j=1,2,\cdots,s$，由于这些点的轮数都小于 $s+1$，因此显然有 $i_j<k-1$。

引理 8.2.5

(1) 设 $r=\frac{a}{b}, b>0,(a,b)=1$ 是一个有理数，$x_n=\{nr\}$。x_{k-1},x_k 是两个相邻的点。如果 $x_k-x_{k-1}>\frac{1}{b}$，那么必存在无穷多个整数 $n_1<n_2<\cdots$ 使得 $x_{n_i}\in(x_{k-1},x_k)$。

(2) (1) 设 θ 是一个无理数，$x_n=\{n\theta\}$。x_{k-1},x_k 是两个相邻的点，那么必存在无穷多个整数 $n_1<n_2<\cdots$ 使得 $x_{n_i}\in(x_{k-1},x_k)$。

证明 (1) 设 $x_k-x_{k-1}>\frac{1}{b}$，那么根据定理 8.1.1，在 $x_0,x_1,\cdots,x_{b-1}$ 这 b 个点中必有某个点 $z\in(x_{k-1},x_k)$，又由于叙列 $x_0,x_1,\cdots,x_n,\cdots$ 是周期为 b 的周期叙列（定理 8.1.1），因此必存在无穷多个整数 $n_1<n_2<\cdots$ 使得 $x_{n_i}\in(x_{k-1},x_k)$。

(2) 如果 θ 是一个无理数，那么 $x_0,x_1,\cdots,x_n,\cdots$ 是两两不同的，由 $\{n\theta\}$ 的稠密性即知存在无穷多个整数 $n_1<n_2<\cdots$ 使得 $x_{n_i}\in(x_{k-1},x_k)$。

引理 8.2.6 设 θ 是任意实数，$x_n=\{n\theta\}$。区间 $(0,1)$ 被 $x_1,\cdots,x_{k-1}$ 分成了 k 个子区间，其中包含 x_k 的子区间的长度为 Δ_k，又设区间 $(0,1)$ 被 $x_1,\cdots,x_{k-1},x_k$ 分成了 $k+1$ 个子区间，其中包含 x_{k+1} 的子区间的长度为 Δ_{k+1}，那么必有 $\Delta_{k+1}\leqslant\Delta_k$。

证明 首先定义符号 $⩽\!\!\!\!\bigcirc$ 的含义如下：$x_n ⩽\!\!\!\!\bigcirc x_k$ 表示 (x_n,x_k) 在中不存在任何叙列 $x_1,\cdots,x_n,\cdots$ 中的任何点。其次注意假如有 $x_n ⩽\!\!\!\!\bigcirc x_k ⩽\!\!\!\!\bigcirc x_m$，$x_{n+1} ⩽\!\!\!\!\bigcirc x_{k+1} ⩽\!\!\!\!\bigcirc x_{m+1}$，那么我们可以写 $\Delta_k=x_m-x_n$，却不能写 $\Delta_{k+1}=x_{m+1}-x_{n+1}$，但是可以写 $\Delta_{k+1}\leqslant x_{m+1}-x_{n+1}$。这是因为即使在 (x_n,x_k) 中和 (x_k,x_m) 中都没有分点，但是在 (x_{n+1},x_{k+1}) 和 (x_{k+1},x_{m+1}) 中仍可能存在分点。例如设 $\theta=\frac{7}{51}$，那么我们有

$$x_{15} ⩽\!\!\!\!\bigcirc x_{23} ⩽\!\!\!\!\bigcirc x_{16}, x_{16}<x_2<x_{24}<x_{17}$$

以下分 9 种情况进行讨论：

(1) $x_n ⩽\!\!\!\!\bigcirc x_k ⩽\!\!\!\!\bigcirc x_m, x_{n+1}<x_{k+1}<x_{m+1}$。

这时或者(i) $x_n<x_{n+1}, x_k<x_{k+1}, x_m<x_{m+1}$，或者(ii) $x_{n+1}<x_n, x_{k+1}<x_k, x_{m+1}<x_m$。

如果发生情况(i)，根据引理 8.2.1 就有

$$x_{n+1}=x_n+\{\theta\}, x_{k+1}=x_k+\{\theta\}, x_{m+1}=x_m+\{\theta\}$$

因此
$$\Delta_{k+1}\leqslant x_{m+1}-x_{n+1}=x_m-x_n=\Delta_k$$

如果发生情况(ii)，根据引理 8.2.1 就有

$$x_{n+1}=x_n+\{\theta\}-1, x_{k+1}=x_k+\{\theta\}-1, x_{m+1}=x_m+\{\theta\}-1$$

因此同样有

$$\Delta_{k+1} \leqslant x_{m+1} - x_{n+1} = x_m - x_n = \Delta_k$$

除开以上两种情况,其他情况都是不可能发生的。例如 $x_{n+1} > x_n, x_{k+1} > x_k, x_{m+1} < x_m$ 或 $x_{n+1} > x_n, x_{k+1} < x_k$(这是根据引理 8.2.2 必有 $x_{m+1} < x_m$),否则就有

$$x_{n+1} = x_n + \{\theta\}, x_{k+1} = x_k + \{\theta\}, x_{m+1} = x_m + \{\theta\} - 1$$

那么从 $x_{k+1} < x_{m+1}$ 就得出

$$x_k + \{\theta\} < x_m + \{\theta\} - 1$$

因而 $x_k < x_m - 1 < 0$ 矛盾。同理可以说明 $x_{n+1} > x_n, x_{k+1} < x_k$ 也不可能发生。

(2) $x_n \olessthan x_k \olessthan x_m, x_{n+1} < x_{k+1} < 1$。

这时必有 $x_{m+1} < x_m$。否则由引理 8.2.1 就有

$$x_n < x_{n+1}, x_k < x_{k+1}, x_m < x_{m+1}$$

$$x_{n+1} = x_n + \{\theta\}, x_{k+1} = x_k + \{\theta\}, x_{m+1} = x_m + \{\theta\}$$

因而 $x_{n+1} < x_{k+1} < x_{m+1}$,这就化为(1)中(i)已证明过的情况。因此只须考虑情况 $x_m + \{\theta\} > 1$,因而根据引理 8.2.1 $x_{m+1} = x_m + \{\theta\} - 1$ 的情况。这时

$$\Delta_{k+1} \leqslant 1 - x_{n+1} \leqslant 1 - x_n - \{\theta\} \leqslant x_m - x_n \leqslant \Delta_k$$

(3) $x_n \olessthan x_k \olessthan x_m, 0 < x_{k+1} < x_{m+1}$。

这时必有 $x_n < x_{n+1}$。否则由根据引理 8.2.1 得出

$$x_{n+1} < x_n, x_{k+1} < x_k, x_{m+1} < x_m$$

$$x_{n+1} = x_n + \{\theta\} - 1, x_{k+1} = x_k + \{\theta\} - 1, x_{m+1} = x_m + \{\theta\} - 1$$

因而 $x_{n+1} < x_{k+1} < x_{m+1}$,这就又化为(1)中(i)已证明过的情况。因此只须考虑情况 $x_{n+1} = x_n + \{\theta\} < 1$。这时

$$\Delta_{k+1} \leqslant x_{m+1} \leqslant x_m + \{\theta\} - 1 \leqslant x_m - x_n \leqslant \Delta_k$$

(4) $x_n \olessthan x_k \olessthan 1, x_n < x_{n+1} < x_{k+1} < 1$。

这时

$$x_{n+1} = x_n + \{\theta\}, x_{k+1} = x_k + \{\theta\}$$

$$\Delta_{k+1} \leqslant 1 - x_{n+1} \leqslant 1 - x_n - \{\theta\} \leqslant 1 - x_n \leqslant \Delta_k$$

(5) $x_n \olessthan x_k \olessthan 1, 0 < x_{k+1} < x_k$。

这时

$$0 < x_{k+1} < x_k < x_n < x_{n+1} < 1$$

$$x_{k+1} = x_k + \{\theta\} - 1 < x_k, x_{n+1} = x_n + \{\theta\} < 1$$

因此
$$\Delta_{k+1} \olessthan \{\theta\} \leqslant 1 - x_n \leqslant \Delta_k$$

(6) $x_n \olessthan x_k \olessthan 1, 0 < x_{n+1} < x_n$。

这时由引理 8.2.2 知 $x_{k+1} < x_k$,因此由引理 8.2.1 有

$$x_{n+1} = x_n + \{\theta\} - 1, x_{k+1} = x_k + \{\theta\} - 1$$

因而 $$0 < x_{n+1} < x_{k+1} < \{\theta\}$$

故 $$\Delta_{k+1} \leqslant \{\theta\} - x_{n+1} \leqslant \{\theta\} - (x_n + \{\theta\} - 1) \leqslant 1 - x_n \leqslant \Delta_k$$

(7) $0 \leqslant x_k \leqslant x_m, x_m < x_{m+1}$。

这时必有 $x_k < x_{k+1}$,否则由引理8.2.2得出 $x_{m+1} < x_m$,因此由引理8.2.1知

$$x_{k+1} = x_k + \{\theta\} > \{\theta\}, x_{m+1} = x_m + \{\theta\}$$

故 $$\{\theta\} < x_{k+1} < x_{m+1}$$

而 $$\Delta_{k+1} \leqslant x_{m+1} - \{\theta\} \leqslant x_m + \{\theta\} - \{\theta\} \leqslant x_m \leqslant \Delta_k$$

(8) $0 \leqslant x_k \leqslant x_m, x_k < x_{k+1}, x_{m+1} < x_m$。

这时由引理8.2.1知

$$x_{m+1} = x_m + \{\theta\} - 1 < \{\theta\}, x_{k+1} = x_k + \{\theta\} > \{\theta\}$$

因此 $$x_{m+1} < \{\theta\} < x_{k+1} < 1$$

而 $$\Delta_{k+1} \leqslant 1 - \{\theta\} < x_m \leqslant \Delta_k$$

(9) $0 \leqslant x_k \leqslant x_m, x_{k+1} < x_k$。

这时由引理8.2.2知 $x_{m+1} < x_m$,再由引理8.2.1得

$$x_{k+1} = x_k + \{\theta\} - 1, x_{m+1} = x_m + \{\theta\} - 1$$

因此 $$0 < x_{k+1} < x_{m+1}$$

而 $$\Delta_{k+1} \leqslant x_{m+1} < x_m \leqslant \Delta_k$$

综合以上几种情况就证明了引理。

引理8.2.7 设 θ 是任意实数,$x_n = \{n\theta\}$。区间(0,1)被 $x_1, \cdots, x_{n-1}$ 分成了 n 个子区间,其中包含 x_n 的子区间的长度为 Δ_n,又设区间(0,1)被 $x_1, \cdots, x_{n-1}, x_n$ 分成了 $n+1$ 个子区间,其中包含 x_{n+1} 的子区间的长度为 Δ_{n+1}。如果 $\Delta_{n+1} < \Delta_n$,那么

(1) 在(0,1)被 $x_1, \cdots, x_{n-1}$ 分成了 n 个小区间中,仅有一个小区间的长度等于 Δ_n;

(2) 在(0,1)被 $x_1, \cdots, x_{n-1}$ 分成了 n 个小区间中不存在长度大于 Δ_n 的小区间。

证明 由于 $\Delta_{n+1} < \Delta_n$,因此在 $\theta = \frac{a}{b}, b > 0, (a, b) = 1$ 的情况下必有 $\frac{1}{b} \leqslant \Delta_{n+1} < \Delta_n$,故引理8.2.5成立。

(1) 假设引理不成立,即假设在(0,1)被 $x_1, \cdots, x_{n-1}$ 分成了 n 个小区间中,至少有两个小区间的长度等于 Δ_n;按照 Δ_n 的定义,在这两个小区间中必有一个且仅有一个小区间包含 x_n,用 J 表示这两个小区间中不含 x_n 的那个小区间,于是按照假设和区间 J 的定义就有 $|J| = \Delta_n$。

根据引理 8.2.6，J 不可能包含所有脚标大于 n 的 x_i，即不可能包含 x_{n+1} 本身及其以后的各项 $x_{n+1}, x_{n+2}, \cdots$ 否则按照 Δ_i 的定义将有 $\Delta_n = |J| \leqslant \cdots \leqslant \Delta_{n+2} \leqslant \Delta_{n+1} < \Delta_n$，矛盾。这也就是说 J 只包含 $x_1, \cdots, x_n, \cdots$ 中的有限项，而这又与引理 8.2.5 矛盾。

(2) 假设在 $(0,1)$ 被 $x_1, \cdots, x_{n-1}$ 分成了的 n 个小区间中，存在长度大于 Δ_n 的区间 J，那么与(1)类似，J 不可能包含所有脚标大于 n 的 x_i，即不可能包含 x_{n+1} 本身及其以后的各项 $x_{n+1}, x_{n+2}, \cdots$ 否则按照 Δ_i 的定义将有 $\Delta_n < |J| \leqslant \cdots \leqslant \Delta_{n+2} \leqslant \Delta_{n+1} < \Delta_n$，矛盾。这也就是说 J 只包含 $x_1, \cdots, x_n, \cdots$ 中的有限项，而这又与引理 8.2.5 矛盾。

下面我们就来证明这一节的主要结果。

定理 8.2.1 设 θ 是任意实数，$x_n = \{n\{\theta\}\}$。区间 $(0,1)$ 被 $x_1, \cdots, x_{n-1}$ 分成了 n 个区间，那么这 n 个区间的长度至多有 3 个值，如果这 n 个区间的长度有 3 个值，那么它们之中的最大值必等于另外两个值之和。

证明 当 $0 < \{\theta\} < \frac{1}{2}$ 时，对 $n = 1,2,\cdots,\left[\frac{1}{\{\theta\}}\right]$，可直接验证小区间的长度只有两个值 x_1 和 $1 - x_n$，因此定理成立。

对 $n = \left[\frac{1}{\{\theta\}}\right] + 1$，由 $\left[\frac{1}{\{\theta\}}\right] \leqslant \frac{1}{\{\theta\}} < \left[\frac{1}{\{\theta\}}\right] + 1$ 可知 $x_{n-1} < 1, x_{n-1} + \{\theta\} > 1$，因此

$$0 < x_n < x_1 < x_2 < \cdots < x_{n-1} < 1$$

而
$$x_n = x_{n-1} + \{\theta\} - 1$$

$$x_1 - x_n = x_1 - (x_{n-1} + \{\theta\} - 1) = x_1 - (x_{n-1} - x_1 - 1) = 1 - x_{n-1}$$

因此 $I = [0,1]$ 被 $x_1, x_2, \cdots, x_n$ 所分成的 $n + 1$ 个区间的长度共有 3 个值

$$x_1 = |(x_1, x_2)| = |(x_2, x_3)| = \cdots = |(x_{n-2}, x_{n-1})|$$

$$1 - x_{n-1} = |(x_n, x_1)| = |(x_{n-1}, 1)|$$

和
$$x_n = |(0, x_n)|$$

由
$$x_{n-1} = (n-1)\{\theta\} < 1 < x_{n-1} + \{\theta\}$$

得出
$$1 - x_{n-1} < \{\theta\} \leqslant x_1, x_n < \{\theta\} \leqslant x_1$$

因此这 3 种长度中最大者为恰为 $x_1 = (1 - x_{n-1}) + x_n$，恰为其他两种长度之和，因此这时定理也是成立的。

当 $\{\theta\} = \frac{1}{2}$ 时，定理显然成立。

当 $\{\theta\} > \frac{1}{2}$ 时，对 $n = 1,2,\cdots,\left[\frac{1}{1 - \{\theta\}}\right]$ 有 $0 < x_n < x_{n-1} < \cdots < x_2 < x_1 < 1$，而

$$x_2 = x_1 + \{\theta\} - 1 = x_1 + x_1 - 1 = 2x_1 - 1$$

$$x_3 = x_2 + \{\theta\} - 1 = 2x_1 - 1 + x_1 - 1 = 3x_1 - 2$$

$$\vdots$$

$$x_n = x_{n-1} + \{\theta\} - 1 = (n-1)x_1 - (n-2) + x_1 - 1 = nx_1 - (n-1)$$

这时小区间的长度共有两个值

$$1 - x_1 = |(x_n, x_{n-1})| = \cdots = |(x_2, x_1)| = |(x_1, 1)|$$

和
$$x_n = |(0, x_n)|$$

因此这时定理成立。

对 $n = \left[\frac{1}{1 - \{\theta\}}\right] + 1$,有

$$n - 1 \leqslant \left[\frac{1}{1 - \{\theta\}}\right] \leqslant \frac{1}{1 - \{\theta\}} < \left[\frac{1}{1 - \{\theta\}}\right] + 1 \leqslant n$$

及
$$x_{n-1} = (n-1)x_1 - (n-2) > 0$$

因而有
$$(n-1)(1 - \{\theta\}) \leqslant 1 < n(1 - \{\theta\})$$

或
$$(n-1) - (n-1)\{\theta\} \leqslant 1 < n - n\{\theta\}$$

也就是
$$n - 2 \leqslant (n-1)\{\theta\} < n\{\theta\} < n - 1$$

故必有

$$x_n = \{n\{\theta\}\} = n\{\theta\} - (n-2) = nx_1 - (n-2)$$

$$0 < x_{n-1} < x_{n-2} < \cdots < x_1 < x_n < 1$$

由于

$$x_n - x_1 = x_{n-1} + \{\theta\} - x_1 = x_{n-1}$$

因此 $I = [0,1]$ 被 $x_1, x_2, \cdots, x_n$ 所分成 $n+1$ 个区间的长度共有 3 个值

$$1 - x_1 = |(x_{n-1}, x_{n-2})| = |(x_{n-2}, x_{n-3})| = \cdots = |(x_2, x_1)|$$

$$x_{n-1} = |(0, x_{n-1})| = |(x_1, x_n)|$$

和
$$1 - x_n = |(x_n, 1)|$$

由
$$x_{n-1} < x_1 < x_n, x_n - x_1 = x_{n-1}$$

得出
$$1 - x_n < 1 - x_1, x_{n-1} < 1 - x_1$$

故 $1 - x_1$ 是这 3 种长度中最大的,而

$$1 - x_1 = x_{n-1} + (1 - (x_{n-1} + x_1)) = x_{n-1} + (1 - x_n)$$

恰为其他两种长度之和。因此这时定理也是成立的。

下面我们用数学归纳法证明定理。

假设对 $2 \leqslant k \leqslant n$ 的所有自然数 k,定理成立。又设区间 $I = [0,1]$ 被 $x_1, x_2, \cdots, x_n$ 分成了 $n+1$ 个小区间。

以下分情况进行讨论。

1. 在上述 $n+1$ 个小区间中存在两个相邻的区间 (x_k, x_n) 和 $(x_n, 1)$,其中 $k < n$。这时又分两种情况:

(1) $k < n - 1$。

由于 x_{k+1} 不在 x_k 和 1 之间，因此它一定跑到下一轮去了，也就是说 $(k + 1)|\theta| > 1$，故由 8.2.1 可知

$$x_{k+1} = (k + 1)|\theta| - 1$$

又由于 $k < n$，故

$$(n + 1)|\theta| > 1, x_{n+1} = (n + 1)|\theta| - 1$$

而由于 x_n 在 x_k 和 1 之间，故 $x_n = n|\theta| < 1$，从而

$$x_{n+1} = (n + 1)|\theta| - 1 < |\theta|$$

这就得出

$$0 < x_{k+1} < x_{n+1} < x_1 < x_k < x_n < 1$$

对 $m = 2,3,\cdots,n$，显然有 $m \neq n + 1$，因此 x_m 不可能位于 x_{k+1} 和 x_1 之间，否则 x_{m-1} 将在 x_k 和 1 之间，而这与 x_k 和 1 之间仅包含分点 x_n 相矛盾。

由归纳法假设可知区间 $I = [0,1]$ 被 $x_1, x_2, \cdots, x_n$ 所分成 $n + 1$ 的个小区间至多有 3 种长度

$$x_n - x_k = |(x_k, x_n)|, 1 - x_n = |(x_n, 1)|, 1 - x_k = |(x_{k+1}, x_1)|$$

增加了分点 x_{n+1} 后，产生了两个新的小区间 (x_{k+1}, x_{n+1}) 和 (x_{n+1}, x_1)，由计算可知

$$|(x_{k+1}, x_{n+1})| = x_{n+1} - x_{k+1} = (x_n + |\theta| - 1) - (x_k + |\theta| - 1) = x_n - x_k$$

$$|(x_{n+1}, x_1| = x_1 - x_{n+1} = x_1 - (x_n + |\theta| - 1) = 1 - x_n$$

因此增加分点 x_{n+1} 后，$I = [0,1]$ 被 $x_1, x_2, \cdots, x_n, x_{n+1}$ 所分成的 $n + 2$ 个小区间的长度种类并没有增加，这就证明了定理对自然数 $n + 1$ 仍然成立。

(2) $k = n - 1$。

这时

$$0 < x_1 < x_2 < \cdots < x_{n-1} < x_n < 1$$

区间 $I = [0,1]$ 被 $x_1, x_2, \cdots, x_n$ 所分成的 $n + 1$ 个小区间的最右边的两个区间是 (x_{n-1}, x_n) 和 $(x_n, 1)$，而这 $n + 1$ 个小区间的的长度只有两种：x_1 和 $1 - x_n$。当增加分点 x_{n+1} 后，有可能发生以下 3 种情况：

(i) $(n + 1)|\theta| < 1$。这时

$$0 < x_1 < x_2 < \cdots < x_{n-1} < x_n < x_{n+1} < 1$$

因此 $I = [0,1]$ 被 $x_1, x_2, \cdots, x_n, x_{n+1}$ 所分成的 $n + 2$ 个小区间的长度仍只有两种 x_1 和 $1 - x_{n+1}$。

(ii) $(n + 1)|\theta| > 1$。这时增加分点 x_{n+1} 后，$x_{n+1} = 0$。定理显然成立。

(iii) $(n + 1)|\theta| > 1$。

由引理 8.2.1 和 8.2.2 知

$$x_n = n\{\theta\} < 1, x_{n+1} = (n+1)\{\theta\} - 1 = \{\theta\} + n\{\theta\} - 1 < \{\theta\}$$

故
$$0 < x_{n+1} < x_1 < x_2 < \cdots < x_n < 1$$

由直接计算可知

$$|(x_{n+1}, x_1)| = x_1 - x_{n+1} = x_1 - (x_n + \{\theta\} - 1) = 1 - x_n$$

因此 $I = [0,1]$ 被 $x_1, x_2, \cdots, x_n, x_{n+1}$ 所分成的 $n+2$ 个小区间的长度至多有 3 种：x_1，$1 - x_n$ 和 x_{n+1}。显然 $x_{n+1} < x_1$，$1 - x_n < x_1$，因此这 3 种长度中最大者为

$$x_1 = 1 - x_n + (x_n + \{\theta\} - 1) = (1 - x_n) + x_{n+1}$$

恰为其他两种长度之和。

因此无论发生哪种情况，定理对自然数 $n+1$ 仍然成立。

2. 区间 $I = [0,1]$ 被 $x_1, x_2, \cdots, x_n$ 所分成 $n+1$ 的个小区间的最左边的两个区间是 $(0, x_n)$ 和 (x_n, x_k)，其中 $k < n$。这时又分两种情况：

(1) $k < n - 1$。

由于 x_{k-1} 不在 0 和 x_k 之间，故由引理 8.2.1 和 8.2.2 知 $x_{k-1} + \{\theta\} > 1$，$x_n < x_k = x_{k-1} + \{\theta\} - 1$ 或者 $k = 1$。又由于 x_{k+1} 不在 0 和 x_k 之间，故由引理 8.2.1 和 8.2.2 知

$$x_n + \{\theta\} < x_k + \{\theta\} < 1, x_{k+1} = x_k + \{\theta\} > x_k, x_{n+1} = x_n + \{\theta\} > x_n$$

对 $m = 2, 3, \cdots, n$，显然 $m \neq n+1$。因此 x_m 必不在 x_1 和 x_{k+1} 之间，否则 x_{m-1} 将在 0 和 x_k 之间，而这与 0 和 x_k 之间仅包含一个分点 x_n 相矛盾。因此只可能发生以下两种情况之一：

(i) $0 < x_n < x_k < x_1 < x_{k+1} < 1$。

这是由于在 0 和 x_1 之间仅包含一个适合 $1 < k < n$ 的点 x_k，因此 x_k 必位于第二轮中。同样由于在 0 和 x_k 之间仅包含一个适合 $n > k$ 的分点 x_n，因此 x_n 必位于第三轮中。由引理 8.2.3 可知 x_k 和 x_n 具有表达式 $x_k = k\{\theta\} - 1$，$x_n = n\{\theta\} - 2$。情况(i)中共可能产生 4 种长度，即 x_n，$x_k - x_n$，$x_1 - x_k$ 和 $x_{k+1} - x_1 = x_k$。然而由归纳法假设，这 4 种长度之中至多有 3 种是不同的，于是必然成立以下 6 个等式之一，即

$$x_n = x_k - x_n \tag{①}$$

$$x_n = x_1 - x_k \tag{②}$$

$$x_n = x_k \tag{③}$$

$$x_k - x_n = x_1 - x_k \tag{④}$$

$$x_k - x_n = x_k \tag{⑤}$$

$$x_1 - x_k = x_k \tag{⑥}$$

显然③、⑤两式不可能成立。如果成立等式①或②，则由上述的 x_k 和 x_n 的表达式易得

$$|\theta| = \frac{3}{N}, N \equiv 1 (\bmod 3)$$

（如果 $N \equiv 2(\bmod 3)$，则易于看出 $x_k = \frac{1}{N}$，不可能成立式 ① 或 ②）

这时易证 $I = [0,1]$ 被 $x_1, x_2, \cdots, x_n$ 所分成的 $n+1$ 个小区间只有两种长度 $\frac{1}{N}$ 或 $\frac{2}{N}$。添加分点 x_{n+1} 后，$I = [0,1]$ 被 $x_1, x_2, \cdots, x_n, x_{n+1}$ 所分成的 $n+2$ 个小区间的长度仍然只是 $\frac{1}{N}$ 或 $\frac{2}{N}$，因此定理对自然数 $n+1$ 也成立。

如果成立等式 ⑥，则由 x_k 和 x_n 的表达式易得 $|\theta| = \frac{2}{2k-1}$，这时 $x_k = \frac{1}{2k-1}$，因此在 0 和 x_k 之间不可能存在分点 x_n，这与假设不符，因此等式 ⑥ 在情况(i) 中不可能出现。

最后只须讨论等式 ④ 成立的情况，这时 $x_k - x_n = x_1 - x_k$。

由于 x_{n+1} 位于 x_1 和 x_{k+1} 之间，因此增添了分点 x_{n+1} 之后，$x_1, x_2, \cdots, x_n, x_{n+1}$ 把 $I = [0,1]$ 所分成 $n+2$ 的个小区间中产生的新的小区间为 (x_1, x_{n+1}) 和 (x_{n+1}, x_{k+1})，而

$$|(x_1, x_{n+1})| = x_{n+1} - x_1 = x_n,\ |(x_{n+1}, x_{k+1})| = x_{k+1} - x_{n+1} = x_k - x_n$$

因此新产生的小区间的长度种类并没有增加，故定理对自然数 $n+1$ 仍然成立。

(ii) $0 < x_n < x_1 < x_2 < 1$。

在这种情况中，由归纳法假设知 $x_1, x_2, \cdots, x_n$，把 $I = [0,1]$ 所分成的 $n+1$ 个小区间中至多存在 3 种长度 x_n，$x_1 - x_n$ 和 $x_2 - x_1 = x_1$。由于 x_{n+1} 位于 x_1 和 x_2 之间，因此增添了分点 x_{n+1} 之后，$x_1, x_2, \cdots, x_n, x_{n+1}$ 把 $I = [0,1]$ 所分成的 $n+2$ 个小区间中产生的新的小区间为 (x_1, x_{n+1}) 和 (x_{n+1}, x_2)。而

$$|(x_1, x_{n+1})| = x_{n+1} - x_1 = x_n$$

$$|(x_{n+1}, x_2)| = x_2 - x_{n+1} = 2x_1 - (x_n + x_1) = x_1 - x_n$$

因此新产生的小区间的长度种类并没有增加，故定理对自然数 $n+1$ 仍然成立。

(2) $k = n - 1$。

这时 $x_1, x_2, \cdots, x_n$ 把 $I = [0,1]$ 所分成的 $n+1$ 个小区间中最左边的两个相邻的小区间为 $(0, x_n)$ 和 (x_n, x_{n-1})。由于 $(0, x_n)$ 和 (x_n, x_{n-1}) 之间都不存在任何分点，故 $x_{n-2} > x_{n-1}$，在 (x_{n-1}, x_{n-2}) 之间也不可能存在任何分点，否则 (x_n, x_{n-1}) 之间将存在分点。因此 $x_{n-3} > x_{n-2}, \cdots$ 依次类推可得

$$0 < x_n < x_{n-1} < x_{n-2} < \cdots < x_1 < 1$$

这时 $x_1, x_2, \cdots, x_n$ 把 $I = [0,1]$ 所分成的 $n+1$ 个小区间共有两种长度 x_n 和 $1 - x_1$，增加分点 x_{n+1} 后，可能出下以下 3 种情况：

(i) $x_n + \{\theta\} > 1$。

这时 $x_{n+1} = x_n + \{\theta\} - 1 < x$,因而 $x_1, x_2, \cdots, x_n, x_{n+1}$ 把 $I = [0,1]$ 所分成的 $n+2$ 个小区间的长度仍为两种:x_{n+1} 和 $1 - x_1$。故定理对于自然数 $n+1$ 仍然成立。

(ii) $x_n + \{\theta\} = 1$。

这时 $\{\theta\} = \dfrac{1}{n}$,易证定理成立。

(iii) $x_n + \{\theta\} = 1$。

这时 $x_{n+1} = x_n + \{\theta\} > x_1$,增添分点 x_{n+1} 后,新产生两个小区间 (x_1, x_{n+1}) 和 $(x_{n+1}, 1)$。而

$$|(x_1, x_{n+1})| = x_{n+1} - x_1 = x_n, \; |(x_{n+1}, 1)| = 1 - x_{n+1}$$

因此 $x_1, x_2, \cdots, x_n, x_{n+1}$ 把 $I = [0,1]$ 所分成的 $n+2$ 个小区间共存在 3 种长度 $x_n, 1 - x_1$ 和 $1 - x_{n+1}$。显然 $1 - x_{n+1} < 1 - x_1, x_n < 1 - x_1$,因此这 3 种长度中最大者为

$$1 - x_1 = x_n + (1 - (x_n + x_1)) = x_n + (1 - x_{n+1})$$

恰为其他两种长度之和。

3. $I = [0,1]$ 被 $x_1, x_2, \cdots, x_n$ 所分成的 $n+1$ 个小区间中存在两个相邻的小区间 (x_m, x_n) 和 (x_n, x_k)。

(1) $m, k < n - 1$。

这时又分以下 3 种情况:

(i) $x_k + \{\theta\} < 1$。

这时因此有 $x_m + \{\theta\} < x_n + \{\theta\} < x_k + \{\theta\} < 1$,因而由引理 8.2.1 和引理 8.2.2 即得

$$x_{m+1} = x_m + \{\theta\}, x_{n+1} = x_n + \{\theta\}, x_{k+1} = x_k + \{\theta\}$$

这也就是说 $x_{m+1}, x_{n+1}, x_{k+1}$ 都分别位于 x_m, x_n, x_k 的右边。

如果 $x_{m+1} < x_k$,那么在 x_m 和 x_k 之间将存在一个分点 x_{m+1}, $m+1 < n$,因此 $x_{m+1} \neq x_n$,而这与 (x_m, x_n) 和 (x_n, x_k) 是相邻小区的假设矛盾,因此必有 $x_{m+1} > x_k$。由归纳法假设,$x_1, x_2, \cdots, x_k$ 把 $I = [0,1]$ 所分成的 $n+1$ 个小区间至多有 3 种长度 $x_n - x_m, x_k - x_n$ 和 $x_{m+1} - x_k$。

增添分点 x_{n+1} 之后,将产生两个新的小区间 (x_{m+1}, x_{n+1}) 和 (x_{n+1}, x_{k+1})。由于

$$|(x_{m+1}, x_{n+1})| = x_{n+1} - x_{m+1} = x_n - x_m$$

$$|(x_{n+1}, x_{k+1})| = x_{k+1} - x_{n+1} = x_k - x_n$$

因此增添分 x_{n+1} 点后,并未产生新的长度,定理对自然数 $n+1$ 仍然成立。

(ii) $x_m + \{\theta\} > 1$。

那么这时有 $x_k+\{\theta\}>x_n+\{\theta\}>x_m+\{\theta\}>1$，因此

$$x_{m+1}=x_m+\{\theta\}-1,x_{n+1}=x_n+\{\theta\}-1,x_{k+1}=x_k+\{\theta\}-1$$

x_{k+1} 不可能位于区间(x_m,x_k)之中（由于(x_m,x_k)之中只有一个分点 x_n，而 $k+1<n$，故 $x_{k+1}\neq x_n$），因此必有

$$0<x_{m+1}<x_{n+1}<x_{k+1}<x_m<x_n<x_{k+1}<1$$

用与情况(i)中相同的论证方法就可得出定理对自然数 $n+1$ 仍然成立。

(iii) $x_n+\{\theta\}<1,x_k+\{\theta\}>1$。

这时因此

$$x_m+\{\theta\}<x_n+\{\theta\}<1,x_{m+1}=x_m+\{\theta\}$$

$$x_{n+1}=x_n+\{\theta\},x_{k+1}=x_k+\{\theta\}-1$$

且 x_{k+1} 不能在区间(x_m,x_k)之中（由于(x_m,x_k)之中只有一个分点 x_n，而 $k+1<n$；故 $x_{k+1}\neq x_n$）。

设 x_k 位于第 s 轮，又设 n_1 是第一轮的最后一个元素，则

$$n_1\{\theta\}<1,(n_1+1)\{\theta\}>1,x_{k-1}=(k-1)\{\theta\}-s+1,x_k=k\{\theta\}-s+1$$

由此易证 $x_{k-1}<x_{k+n_1}<x_k$。

由于(x_m,x_n)和(x_n,x_k)是两个相邻的小区间，因此 x_{k-1} 不可能位于上述两个小区间之中，因而只能有 $x_{k-1}\leqslant x_m$。如果 $x_{k-1}<x_m$，那么这就必有 $x_m+\{\theta\}>1$（否则由于 $x_{k-1}<x_m$，那么在$(x_k,1)$之间将有分点 x_{m+1}），这就又化为(ii)中已证明过的情况了。

如果 $x_{k-1}=x_m$，那么 x_{k-1},x_k 必属于第一轮，x_n 必属于第二轮。否则由引理 8.2.4 知(x_{k-1},x_k)中必含有一个分点 x_h，$h<k-1$，这与(x_{k-1},x_k)中仅含有一个分点 x_n，$k<n$ 矛盾。

由 x_{k-1},x_k 属于第一轮可得$k\{\theta\}<1,(k+1)\{\theta\}>1,x_{k-1}=(k-1)\{\theta\}$，$x_k=k\{\theta\}$。

易证 $x_{k-1}<x_{2k}<x_k$ 以及 $x_1,x_2,\cdots,x_n$ 把 $I=[0,1]$ 所分成的 $n+1$ 个小区间共有两种长度

$$1-x_k=x_k-x_n=1-k\{\theta\}$$

和

$$\{\theta\}-(1-k\{\theta\})=(k+1)\{\theta\}-1$$

因此

$$x_n=x_k-(1-k\{\theta\})=k\{\theta\}-(1-k\{\theta\})=2k\{\theta\}-1$$

$$x_{n+1}=x_n+\{\theta\}=(2k+1)\{\theta\}-1$$

增添分点 x_{n+1} 后，将产生两个新的小区间(x_k,x_{n+1})和$(x_{n+1},1)$，而

$$|(x_k,x_{n+1})|=x_{n+1}-x_k=(k+1)\{\theta\}$$

$$|(x_{n+1},1)|=1-x_{n+1}=1-((2k+1)\{\theta\}-1)=2-(2k+1)\{\theta\}$$

因此 $x_1,x_2,\cdots,x_n,x_{n+1}$ 把 $I=[0,1]$ 所分成的 $n+2$ 个小区间共存在 3 种长度

$$1-k\{\theta\},(k+1)\{\theta\}-1,2-(2k+1)\{\theta\}$$

且按上述假设 $1-x_{n+1}=2-(2k+1)\{\theta\}>0$,因此最长的长度是

$$1-k\{\theta\}=(k+1)\{\theta\}-1+2-(2k+1)\{\theta\}$$

恰为其他两种长度之和。故定理对自然数 $n+1$ 也成立。

理论上还可能发生以下情况:

(2) $m=n-1,k<n-1$。

(3) $k=n-1,m<n-1$。这时

$$0<x_m<x_n<x_{n-1}<x_{m-1}<1$$

我们证明这两种情况都不可能发生。

在情况(2)中,如果 $k=1$,那么 $\{\theta\}=x_n-x_{n-1}<x_k=x_1=\{\theta\}$,矛盾。

如果 $k>1$,那么又分两种情况:

(i) $x_k<x_{k-1}$。

这时 $\{\theta\}=x_n-x_{n-1}<x_k=x_{k-1}+\{\theta\}-1<\{\theta\}$,矛盾。

(ii) $x_{k-1}<x_k$。

由于在 x_{n-1} 和 x_n 之间没有其他分点,因此必有 $x_{k-1}<x_{n-1}$。这时

$$\{\theta\}=x_n-x_{n-1}<x_k-x_{k-1}=\{\theta\}$$

矛盾。

因此情况(2)不可能发生。

在情况(3)中,如果 $m=1$,那么 $\{\theta\}=x_1=x_m<x_n=x_{n-1}+\{\theta\}-1<\{\theta\}$,矛盾。

如果 $m>1$,那么又分两种情况:

(i) $x_m<x_{m-1}$。

由于在 x_m 和 x_n 之间没有其他分点,因此必有 $x_{n-1}<x_{m-1}$,这时

$$x_n=x_{n-1}+\{\theta\}-1,x_m=x_{m-1}+\{\theta\}-1$$

因而 $1-\{\theta\}=x_{n+1}-x_n<x_{m-1}-x_m=1-\{\theta\}$,矛盾。

(ii) $x_{m-1}<x_m$。

这时

$$0<x_{m-1}<x_m<x_n<x_{n-1}<1$$

因而 $\{\theta\}=x_m-x_{m-1}<x_m<x_n=x_{n-1}+\{\theta\}-1<\{\theta\}$,矛盾。
因此情况(3)也不可能发生。

综合以上各种情况,由数学归纳法就证明了定理。

习题 8.2

1. 对 $\theta=\sqrt{2}-1$ 和 $\theta=\frac{\sqrt{5}-1}{2}$ 以及 $n=1,2,\cdots,20$ 验证定理 8.2.1。并对

每一个 n 的值，算出 $x_1, x_2, \cdots, x_n, x_i = |i(\theta)|$ 这 n 个点把区间 $I = [0,1]$ 所分成 $n+1$ 的个小区间所产生不同的长度，并把这些长度按从小到大的顺序排列出来，列成一个 20 行的表。

2. 设 $\tau = \dfrac{\sqrt{5}-1}{2}$ 是黄金分割比例。在一个周长为 1 的圆周上从任意一点 A_1 开始，按顺时针方向或逆时针方向在圆周上每经过弧长为 τ 的一段弧就标记一点，这样我们就得到圆周上用这种方法所得到的分点的一个叙列：$A_1, A_2, \cdots, A_n, \cdots$。

证明：两个相邻的分点的脚标的差的绝对值必定是一个斐波那契数。

复数

第九章

9.1 复数及其几何意义

复数产生的最初动机是让方程 $x^2+1=0$ 可以有解。定义一个符号 $i=\sqrt{-1}$。符号 i 具有性质 $i^2=-1$。于是 $x^2+1=0$ 有两个解 $x=i$ 和 $x=-i$。如果事情仅是如此，便也就如此而已了。然而奇妙的是，最初为了使 $x^2+1=0$ 有解而创造出来的符号 i 一旦出现，人们就发现，它的用途决不是如此而已。首先，有了这个符号之后，不但当初那个最简单的二次方程 $x^2+1=0$ 可以有解，而且一切代数方程的解都可以用这一个符号表达就够了。由此而产生出来的一系列应用更是当初创立这一符号的人所不可能想到的。

大数学家高斯最先使用了复数这一词汇，并应用复数作出了许多优秀的成果。如果说，一开始，还有很多人由于在 i 这个符号怎么会有意义（因为 $\sqrt{-1}$ 在传统的观念中本来就是没有意义的，即使在现在，如果我们限定在实数范围内，它也仍然是没有意义的）这个问题上徘徊不前。那么正是高斯，通过自己的巨大声望和辉煌成果使复数获得了数学界乃至科学界的承认。

高　斯（Gauss，Carl Friedrich，1777—1855），德国数学家、物理学家、天文学家，生于德国不伦瑞克，卒于格丁根.

科学发展到今天，人们对类似复数这样的新概念，已从当初怀疑它的意义是什么而转变为看它是否能获得有意义的应用。用这样的观念再去看复数，你就会觉得复数是现代科学中的一个不可缺少的成分。比如说，仅仅一个代数方程有多少个根的问题，如果不使用复数的概念，就显得毫无规律，或者即使有人发现了什么规律，那么将此规律表达出来也是极为费劲的。如果仅为抬杠，你也可以把一切利用复数而得到的结果"翻译"成为用实数来叙述（只要你不嫌费劲）以"证明"可以不使用"复数"这个没有意义的概念，然而只要你有耐心去"翻译"哪怕是一两个有价值的结果，你就会发现这纯粹是自讨苦吃，这使你感到，即使仅把"复数"当成是一个能使你简洁而快速地达到目的的中间手段，使用它也是太值得了。

定义 9.1.1　设 a,b 表示两个实数，符号 $\alpha = a + bi$ 称为是一个复数。a 称为复数 α 的实部，用 $\mathrm{Re}\,\alpha$ 表示，b 称为复数 α 的虚部，用 $\mathrm{Im}\,\alpha$ 表示。

在平面上取定一个直角坐标系。那么平面上每个点 M 就都可以用一对有序的实数 (a,b) 来表示。从原点 O 向 M 引一段有方向的线段，就得到一个向量，并且我们规定，平面上所有长度相同，互相平行的有向线段都是等同的，这样，我们就可以用一对有序的实数 (a,b) 来表示任何一个平面上的向量。

把复数 $a + bi$ 和向量 $\overrightarrow{OM}$ 对应起来就给出复数 $\alpha = a + bi$ 的一个几何解释，见图 9.1.1。这时，原来坐标系的横轴成为实轴，而原来坐标系的纵轴称为虚轴。

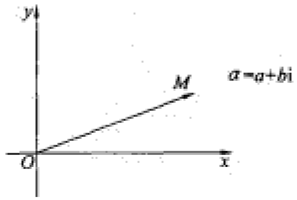


图 9.1.1　复数的几何解释

仅定义了复数概念本身，其意义还不太大，要想使复数获得应用，还必须能对它进行运算，因为数的最重要的特性之一就是它能算。

复数的加减法（实际上只要定义了加法，并且由加法的单位元，即可以定义减法）是比较容易定义的，因为无论从它是一个向量的几何解释，还是把它看成为实部和虚部的合成都应该把整个复数的相加减看成是实部和虚部分别相加减，即认为

$$(a_1 + b_1 i) + (a_2 + b_2 i) \Rightarrow (a_1 + a_2) + (b_1 + b_2) i$$

比较复杂的是乘法。如果抽象地考虑这一问题，首先应该确定的是，两个复数相乘之后仍应该得到一个复数。根据上面我们把复数和向量对应起来的观

点，也就是，两个向量用复数表示后，相乘的结果应该还是一个向量。这也就是说，从两个有序坐标(a_1, b_1)和(a_2, b_2)出发，我们应该能够定义一个映射，它把这两个坐标映为一个新的有序坐标(c_1, c_2)，而新的坐标应该被原来的两个坐标唯一地确定，即新坐标应该是原来的两个坐标的函数，因此可以写成$c_1 = f_1(a_1, b_1, a_2, b_2)$，$c_2 = f_2(a_1, b_1, a_2, b_2)$。其次我们还要考虑，这样定义的乘法是否能继承经典乘法的性质，即是否能成立乘法结合律和乘法与加法之间的分配律，最后，我们还要考虑这样定义的乘法是否可以有任何几何解释或其他有实际意义的解释或应用。

如果单独地考虑上述某一个问题，也许不难给出某些乘法法则，例如，仿效加法那样，可以定义

$$f_1(a_1, b_1, a_2, b_2) = a_1a_2, f_2(a_1, b_1, a_2, b_2) = b_1b_2$$

那么不难验证，这样定义的乘法满足结合律和与加法的分配律。可惜这种乘法却没有任何有意义的解释和应用，当然，你也可以预先从几何的观点定义一种乘法法则，但你无法预先知道，这样定义的法则是否能继承经典乘法的性质。所以，如果要统一地考虑上述问题就是很复杂的了，而且，在我们考虑这一问题时，似乎并没有任何线索。

然而幸运的是，当我们把复数写成$\alpha = a + bi$这种形式，并把i看成一个符号（它本来就是一个符号）时，α就成了i的多项式。而多项式之间是可以相乘的，这就很自然地导致一个法则，即把$\alpha_1 = a_1 + b_1i$和$\alpha_2 = a_2 + b_2i$相乘，应该得到

$$(a_1 + b_1i)(a_2 + b_2i) = a_1a_2 + a_1b_2i + a_2b_1i + b_1b_2i^2 = (a_1a_2 - b_1b_2) + (a_1b_2 + a_2b_1)i$$

也就是说，我们刚才还毫无线索，茫然不知如何定义f_1, f_2的应该是

$$f_1(a_1, b_1, a_2, b_2) = a_1a_2 - b_1b_2, f_2(a_1, b_1, a_2, b_2) = a_1b_2 + a_2b_1$$

这真是踏破铁鞋无觅处，得来全不费功夫。而且看来这是最起码的要求了，所以我们就以此作为复数乘法的定义，至于其他的问题，就只能摸着石头过河，走一步，看一步了。

定义 9.1.2

(1) 实数k数乘一个复数$\alpha = a + bi$意为$k\alpha = ka + kbi$；

(2) 两个复数$\alpha_1 = a_1 + bi$和$\alpha_2 = a_2 + b_2i$的加法定义为

$$\alpha_1 + \alpha_2 = (a_1 + a_2) + (b_1 + b_2)i$$

(3) 两个复数$\alpha_1 = a_1 + b_1i$和$\alpha_2 = a_2 + b_2i$的乘法定义为

$$(a_1 + b_1i)(a_2 + b_2i) = (a_1a_2 - b_1b_2) + (a_1b_2 + a_2b_1)i$$

定义了以上运算之后，下面就该来研究这些运算的性质了，其中我们最关心的问题就是这些运算是否还能保留实数的相应运算的原有性质。结果经过实

际检验之后我们发现可以。这就有点意思了，刚才我们那么担心的问题现在竟都一一化解，而这一切，都只是在定义了一个符号之后，顺着一条自然形成的小路到达的，我们所到达的第一站(运算的性质)就已经展现出我们事先不能预料的奇妙之处了。往下走还会到达那里真是很神秘了。

定理 9.1.1 复数的运算满足以下规律：

(1) 加法交换律：$\alpha+\beta=\beta+\alpha$；

(2) 加法结合律：$(\alpha+\beta)+\gamma=\alpha+(\beta+\gamma)$；

(3) 存在加法单位元：$\alpha+0=\alpha$；

(4) 对每一个复数 α，存在加法的逆元 x，使 $\alpha+x=0(x=-\alpha)$；

(5) 乘法交换律：$\alpha\beta=\beta\alpha$；

(6) 乘法结合律：$(\alpha\beta)\gamma=\alpha(\beta\gamma)$；

(7) 乘法对加法的分配律：$\alpha(\beta+\gamma)=\alpha\beta+\alpha\gamma$；

(8) 存在乘法单位元：$1\cdot\alpha=\alpha$；

(9) 如果 $\alpha=a+b\mathrm{i}\neq 0$，那么 α 存在乘法的逆元 x，使 $\alpha x=1$。($x=\dfrac{1}{\alpha}$，$\dfrac{1}{\alpha}$ 的计算公式见下面的定理 9.1.3)

有了加法逆元之后，就可以定义减法。两个复数 $\alpha_1=a_1+b_1\mathrm{i}$ 和 $\alpha_2=a_2+b_2\mathrm{i}$ 的减法定义为

$$\alpha_1-\alpha_2=\alpha_1+(-\alpha_2)=(a_1-a_2)+(b_1-b_2)\mathrm{i}$$

定义 9.1.3 设 $\alpha=a+b\mathrm{i}$，则称 $a-b\mathrm{i}$ 是 α 的共轭复数，记为 $\overline{\alpha}$。

定理 9.1.2 共轭有以下性质：

(1) 自反性：$\overline{\overline{\alpha}}=\alpha$；

(2) 对加法的分配性：$\overline{\alpha+\beta}=\overline{\alpha}+\overline{\beta}$；

(3) 对乘法的分配性：$\overline{\alpha\beta}=\overline{\alpha}\,\overline{\beta}$。

前面我们已经讲过，建立了一个直角坐标系后，平面上每一个点 $M(a,b)$ 都可以对应于一个复数 $\alpha=a+b\mathrm{i}$，反过来也是如此。而我们在中学里已经知道，平面上的每一个点 $M(a,b)$ 不仅可以用直角坐标来表示，也可以用极坐标表示，也就是可以用 OM 和正 x 轴的夹角 θ 和 OM 的长度 r 来表示，而且同一个点 M 的直角坐标和极坐标之间可以互相换算。

换算的公式可以从图 9.1.2 中容易地看出

$$a=ON=r\cos\theta,b=MN=r\sin\theta$$

反过来有
$$r=\sqrt{a^2+b^2},\tan\theta=\frac{MN}{ON}=\frac{b}{a}$$

利用上面的公式，就可以把一个复数写成所谓的三角形式

$$\alpha=a+b\mathrm{i}=r(\frac{a}{r}+\frac{b}{r}\mathrm{i})=r(\cos\theta+\mathrm{i}\sin\theta)$$

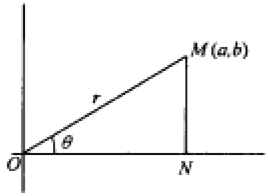


图 9.1.2　复数的三角表示

定义 9.1.4　在复数的三角表示 $\alpha = r(\cos\theta + \mathrm{i}\sin\theta)$ 中，θ 称为是 α 的辐角，记为 $\arg\alpha$，r 称为是 α 的模，记为 $|\alpha|$。

复数 α 的辐角 $\theta = \arg\alpha$ 的几何意义是代表复数 α 的向量与正 x 轴之间的夹角，复数 α 的模 $r = |\alpha|$ 的几何意义是代表复数 α 的向量的长度。

利用复数的共轭，我们可以得出用一个复数来表示模和乘法逆元的公式以及模的乘法性质和辐角的加法性质。

定理 9.1.3

(1) $r^2 = \alpha\overline{\alpha}$；

(2) $\dfrac{1}{\alpha} = \dfrac{\overline{\alpha}}{\alpha\overline{\alpha}} = \dfrac{\overline{\alpha}}{r^2} = \dfrac{a - b\mathrm{i}}{a^2 + b^2}$；

(3) $|k\alpha| = |k||\alpha|$，其中 k 是一个实数；

(4) $|\alpha| = |\overline{\alpha}|$；

(5) $|\alpha\beta| = |\alpha||\beta|$；

(6) $\arg k\alpha = \arg\alpha$；

(7) $\arg\alpha\beta = \arg\alpha + \arg\beta$。

证明　(1)、(2)、(3)、(4) 易证。

现证(5)、(6)、(7)，设 $\alpha_1 = r_1(\cos\theta_1 + \mathrm{i}\sin\theta_1)$，$\alpha_2 = r_2(\cos\theta_2 + \mathrm{i}\sin\theta_2)$，那么

$$\begin{aligned}\alpha_1\alpha_2 = {} & r_1r_2(\cos\theta_1 + \mathrm{i}\sin\theta_1)(\cos\theta_2 + \mathrm{i}\sin\theta_2) = \\ & r_1r_2(\cos\theta_1\cos\theta_1 - \sin\theta_1\sin\theta_2) + \mathrm{i}(\sin\theta_1\cos\theta_2 + \cos\theta_1\sin\theta_2) = \\ & r_1r_2(\cos(\theta_1 + \theta_2) + \mathrm{i}\sin(\theta_1 + \theta_2))\end{aligned}$$

因而有

$$|\alpha\beta| = |\alpha||\beta|, \arg\alpha\beta = \arg\alpha + \arg\beta$$

有了乘法逆元，就可以定义复数的除法

$$\frac{\beta}{\alpha} = \beta\cdot\frac{1}{\alpha} = \frac{\beta\overline{\alpha}}{\alpha\overline{\alpha}}$$

因此有

$$\left|\frac{\beta}{\alpha}\right| = \frac{|\beta|}{|\alpha|}, \alpha \neq 0, \arg\frac{\beta}{\alpha} = \arg\alpha - \arg\beta$$

根据刚才的几何解释，我们从上面这个公式里就可以看出，复数的乘法有以下几何意义：

定理 9.1.4

(1) 要得到任何平行于起点在 α，终点在 β 的向量的复数表示，只要用 β 减去 α 即可；

(2) 起点在 α，方向是 β 的向量的终点的复数表示就是 $\alpha + \beta$；

(3) $\alpha\beta$，即用复数 β 去乘复数 α，是由表示 α 的向量先把原来的长度 $|\alpha|$ 放大(或缩小) $|\beta|$ 倍，再把所得的向量旋转 $\arg\beta$ 角(当 $\arg\beta > 0$ 时，逆时针旋转，当 $\arg\beta < 0$ 时，顺时针旋转) 后所得到的向量。

在上面的乘法公式中令 $\alpha_1 = \alpha_2 = \alpha$ 就得到 $\alpha^2 = r^2(\cos 2\theta + \mathrm{i}\sin 2\theta)$，一般的，就得到

定理 9.1.5(棣莫佛公式) 设 $\alpha = r(\cos\theta + \mathrm{i}\sin\theta)$，则 $\alpha^n = r^n(\cos n\theta + \mathrm{i}\sin n\theta)$。

把 $\mathrm{i}\theta$ 代入到 e^x 的展开式中(即在 e^x 的展开式中令 $x = \mathrm{i}\theta$) 就得到

$$\begin{aligned}\mathrm{e}^{\mathrm{i}\theta} &= 1 + \mathrm{i}\theta + \frac{(\mathrm{i}\theta)^2}{2!} + \frac{(\mathrm{i}\theta)^3}{3!} + \cdots = \\ &1 - \frac{\theta^2}{2!} + \frac{\theta^4}{4!} + \cdots + \frac{(-1)^n\theta^{2n}}{(2n)!} + \cdots + \\ &\mathrm{i}\left(\theta - \frac{\theta^3}{3!} + \frac{\theta^5}{5!} + \cdots + \frac{(-1)^{n+1}\theta^{2n-1}}{(2n-1)!} + \cdots\right) = \\ &\cos\theta + \mathrm{i}\sin\theta\end{aligned}$$

这就是所谓的

定理 9.1.6(欧拉公式) $\mathrm{e}^{\mathrm{i}\theta} = \cos\theta + \mathrm{i}\sin\theta$。

根据欧拉公式，又可把复数的三角表示写成 $\alpha = r(\cos\theta + \mathrm{i}\sin\theta) = r\mathrm{e}^{\mathrm{i}\theta}$，这称为复数的指数表示。

在欧拉公式中令 $\theta = \pi$ 就得到 $\mathrm{e}^{\mathrm{i}\pi} = -1$。

走到这，我们不得不惊叹这个复数真是神奇，它居然神不知鬼不觉地把向量的乘法的定义和经典的乘法统一起来，而且还有明显的几何意义，最后竟然还能把 e 和 π 这两个一开始怎么也看不出来有什么关系的数联系起来，这简直是出神入化，太奇妙了。而当初创立 i 这个符号的人，恐怕怎么也无法想象到从这个 i 出发，会发展出这么一大堆东西来。所以当初难怪大数学家高斯在 1825 年的一封信中也说了"$\sqrt{-1}$ 的真正奥妙是难以捉摸的"这样一句话。连高斯老先生都对 i 的奥妙感到难以捉摸，那我辈是更不用说了。所以这个数学真像一座神秘的殿堂，如果你走错门了，打开门之后就是一个四面都是墙的空屋子，哪也通不到。而如果你走对了门，就会发现屋里还有好多门，如果你又开对了门，进去之后，又有许多门 … 这样一道一道门的一步一步打开，你就会进入一个令

你眼花缭乱，充满了财宝的宝藏。

不过，虽然复数继承了很多实数的原来性质，但是有一个性质却不能继承，那就是顺序性。这个就没有办法了，因为实数的顺序性是一维空间的特有性质。我们说复数不能继承实数的顺序性并不是说对复数不可能规定顺序。实际上，我们有不只一种办法可以规定复数的顺序，比如说，任给两个复数，我们可以规定实部较大的复数较大，而当实部相等时，规定虚部较大的复数较大，不难证明，这样规定的顺序满足以下性质：

(1) 对任意两个复数 α,β，在三个关系式 $\alpha>\beta,\alpha=\beta,\alpha<\beta$ 之中，必有一个且仅有一个成立；

(2) 如果 $\alpha>\beta,\beta>\gamma$，那么 $\alpha>\gamma$。

我们也可以规定任给两个复数，模较大的复数较大，而当模相等时辐角较大的复数较大。可以验证，这样规定的顺序同样满足上面的两条性质。但是又跟我们上面规定的第一种顺序的性质有一个很大的差别，那就是在第二种顺序下，全体复数中存在着一个最小的数，就是零。而实数的顺序下和第一种顺序下，全体实数或复数中是没有最小数的。

既然我们可以给复数规定适当的顺序，那为什么又不给复数定义一种顺序呢？这里的关键问题在于，不管你怎样规定复数的顺序，这种顺序都不可能完全和原来的实数中的顺序协调起来。

定理 9.1.7 复数的任何一种顺序关系都不可能同时满足以下实数原来具有的性质：

(1) 对任意两个复数 α,β，在三个关系式 $\alpha>\beta,\alpha=\beta,\alpha<\beta$ 之中，必有一个且仅有一个成立；

(2) 如果 $\alpha>\beta,\beta>\gamma$，那么 $\alpha>\gamma$；

(3) 如果 $\alpha>0,\beta>0$，那么 $\alpha+\beta>0,\alpha\beta>0$。

证明 根据(1) i 和 0 这两个数，必在 $i>0,i=0,i<0$ 这三个关系中成立一种，且仅成立一种。显然 $i\neq0$，否则我们将得出 $-1=i^2=0$，这显然是一个矛盾。

现在假设 $i>0$，那么根据(3) 就将有 $-1=i^2>0$，得出矛盾。

最后如果 $i<0$，那么 $-i=0-i>0$，因此根据(3) 就将有 $-1=(-i)^2>0$，我们仍然得出矛盾。

因此无论我们如何规定复数之间的顺序，首先 i 和 0 这两个数之间就无法规定顺序，这又和(1) 矛盾。

不过虽然我们不给复数本身规定顺序，复数的模之间却是可以比较大小的。我们有

定理 9.1.8

(1) $||\alpha|-|\beta|| \leqslant |\alpha \pm \beta| \leqslant |\alpha|+|\beta|$（三角不等式）；

(2) $|e^{\alpha}| \leqslant e^{|\alpha|}$。

证明　(1) 如图9.1.3，利用复数的几何意义，把表示β的向量的起点放在表示α的向量的终点上，那么从α的起点指向β终点的向量就表示复数$\alpha+\beta$。而$|\alpha|$，$|\beta|$和$|\alpha+\beta|$就分别表示向量α，β和$\alpha+\beta$的长度。因此由图9.1.3并利用三角形两边之和必不小于第三边的事实就得到

$$|\alpha+\beta| \leqslant |\alpha|+|\beta|$$

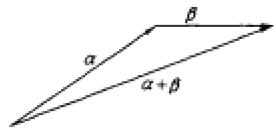


图9.1.3　三角不等式的几何意义

当然你也可以利用复数的定义给出一个代数的证明，这项工作就留给读者自己去做了。

在上面的式子中把β换成$-\beta$就得到

$$|\alpha-\beta| = |\alpha+(-\beta)| \leqslant |\alpha|+|-\beta| = |\alpha|+|\beta|$$

由已证的不等式又可得到

$$|\alpha| = |\alpha-\beta+\beta| \leqslant |\alpha-\beta|+|\beta|$$

因而

$$|\alpha|-|\beta| \leqslant |\alpha-\beta|$$

同理可以得出

$$-(|\alpha|-|\beta|) = |\beta|-|\alpha| \leqslant |\beta-\alpha| = |\alpha-\beta|$$

因而

$$||\alpha|-|\beta|| \leqslant |\alpha \pm \beta| \leqslant |\alpha|+|\beta|$$

(2) 设$\alpha = a+bi$，则$e^{|\alpha|} = e^{\sqrt{a^2+b^2}} \geqslant e^{|a|} \geqslant e^{a} = |e^{a}e^{bi}| = |e^{a+bi}| = |e^{\alpha}|$。

下面我们来看几个例子，从这几个例子中你可以体会到，用复数的"眼睛"看问题，确实会看出一些用实数这个"凡眼"难以看出的联系和方法。

例9.1.1　如图9.1.4，证明：$\angle 1 = \angle 2 + \angle 3$。

证明　以图9.1.4中矩形的底边和左边作为坐标轴，以O为原点建立坐标系，那么在此坐标系中，向量OA，OB和OC可以分别用$\alpha = 1+i$，$\beta = 2+i$和$\gamma = 3+i$来表示。并且从图中可以看出$\angle 1$，$\angle 2$，$\angle 3$分别就是复数α，β，γ的辐角。根据复数的几何意义，我们只须证明$\beta\gamma$（其辐角为$\angle 2+\angle 3$）的辐角等于α（其辐角为$\angle 1$）的辐角即可。

由于

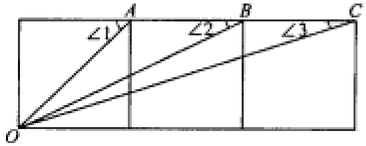


图 9.1.4

$$\beta\gamma = (2+\mathrm{i})(3+\mathrm{i}) = 5(1+\mathrm{i})$$

所以

$$\angle 2 + \angle 3 = \arg\beta + \arg\gamma = \arg\beta\gamma = \arg 5(1+\mathrm{i}) =$$
$$\arg(1+\mathrm{i}) = \arg\alpha = \angle 1$$

这个问题你当然不用复数也可以做出来。那样的路线无非是先要求出来 $\tan\angle 1 = 1, \tan\angle 2 = \frac{1}{2}, \tan\angle 3 = \frac{1}{3}$，然后再得出来 $\angle 2 = \arctan\frac{1}{2}, \angle 3 = \arctan\frac{1}{3}$，再去算 $\tan(\angle 2 + \angle 3)$ 并证明它就等于 $\tan\angle 1$，然后还要说明 $\angle 1$ 以及 $\angle 2 + \angle 3$ 都是锐角，最后才能得出来 $\angle 1 = \angle 2 + \angle 3$。其路线的曲折，手段的繁琐显然要比上面的方法复杂，而且这还只是要证明两个角之和等于另一个角，如果要证 3 个角，4 个角之类的问题，其繁琐程度就可想而知了。

例 9.1.2 求和：$\sin\theta + \sin 2\theta + \cdots + \sin n\theta$。

解 令

$$P = \cos\theta + \cos 2\theta + \cdots + \cos n\theta$$
$$Q = \sin\theta + \sin 2\theta + \cdots + \sin n\theta$$
$$r = \cos\theta + \mathrm{i}\sin\theta$$

则

$$P + Q\mathrm{i} = r + r^2 + \cdots + r^n = r(1 + r + \cdots + r^{n-1}) = \frac{r(1-r^n)}{1-r} =$$
$$\frac{(\cos\theta + \mathrm{i}\sin\theta)(1 - \cos n\theta - \mathrm{i}\sin n\theta)}{1 - \cos\theta - \mathrm{i}\sin\theta} =$$
$$\frac{(\cos\theta + \mathrm{i}\sin\theta)\left(2\sin^2\frac{n\theta}{2} - 2\mathrm{i}\sin\frac{n\theta}{2}\cos\frac{n\theta}{2}\right)}{\left(2\sin^2\frac{\theta}{2} - 2\mathrm{i}\sin\frac{\theta}{2}\cos\frac{\theta}{2}\right)} =$$
$$\frac{\sin\frac{n\theta}{2}}{\sin\frac{\theta}{2}}(\cos\theta + \mathrm{i}\sin\theta)\frac{\left(\sin\frac{n\theta}{2} - \mathrm{i}\cos\frac{n\theta}{2}\right)}{\sin\frac{\theta}{2} - \mathrm{i}\cos\frac{\theta}{2}} =$$
$$\frac{\sin\frac{n\theta}{2}}{\sin\frac{\theta}{2}}(\cos\theta + \mathrm{i}\sin\theta)\left(\sin\frac{n\theta}{2} - \mathrm{i}\cos\frac{n\theta}{2}\right)\left(\sin\frac{\theta}{2} + \mathrm{i}\cos\frac{\theta}{2}\right) =$$

$$\frac{\sin\frac{n\theta}{2}}{\sin\frac{\theta}{2}}(\cos\theta+\mathrm{i}\sin\theta)\left(\sin\frac{n\theta}{2}\sin\frac{\theta}{2}+\cos\frac{n\theta}{2}\cos\frac{\theta}{2}+\right.$$

$$\left.\mathrm{i}\left(\sin\frac{n\theta}{2}\cos\frac{\theta}{2}-\sin\frac{\theta}{2}\cos\frac{n\theta}{2}\right)\right)=$$

$$\frac{\sin\frac{n\theta}{2}}{\sin\frac{\theta}{2}}(\cos\theta+\mathrm{i}\sin\theta)\left(\cos\frac{n-1}{2}\theta+\mathrm{i}\sin\frac{n-1}{2}\right)=$$

$$\frac{\sin\frac{n\theta}{2}}{\sin\frac{\theta}{2}}\left(\cos\frac{n+1}{2}\theta+\mathrm{i}\sin\frac{n+1}{2}\theta\right)$$

对照等式两边的实部和虚部就得到

$$P=\cos\theta+\cos 2\theta+\cdots+\cos n\theta=\frac{\sin\frac{n\theta}{2}\cos\frac{n+1}{2}\theta}{\sin\frac{\theta}{2}}=$$

$$\frac{\frac{1}{2}\left(\sin\left(\frac{n\theta}{2}+\frac{n+1}{2}\theta\right)+\sin\left(\frac{n\theta}{2}-\frac{n+1}{2}\theta\right)\right)}{\sin\frac{\theta}{2}}=$$

$$\frac{\sin\left(n+\frac{1}{2}\right)\theta-\sin\frac{\theta}{2}}{2\sin\frac{\theta}{2}}=\frac{\sin\left(n+\frac{1}{2}\right)\theta}{2\sin\frac{\theta}{2}}-\frac{1}{2}$$

$$Q=\sin\theta+\sin 2\theta+\cdots+\sin n\theta=\frac{\sin\frac{n\theta}{2}\sin\frac{n+1}{2}\theta}{\sin\frac{\theta}{2}}$$

例 9.1.3 证明:三角形两边中点的连线平行于第三边,且是它长度的一半。

证明 如图 9.1.5.

$$\overrightarrow{DE}=\overrightarrow{DC}+\overrightarrow{CE}=\frac{1}{2}\overrightarrow{AC}+\frac{1}{2}\overrightarrow{CB}=$$

$$\frac{1}{2}(\overrightarrow{AC}+\overrightarrow{CB})=\frac{1}{2}\overrightarrow{AB}$$

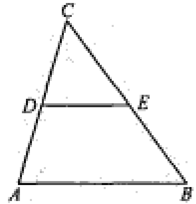


图 9.1.5

因此 $\overrightarrow{DE}\ /\!/\ \overrightarrow{AB}$,且 $|\overrightarrow{DE}|=\frac{1}{2}|\overrightarrow{AB}|$。

例 9.1.4 证明:平行四边形的对角线互相平分。

证明 如图 9.1.6,以下的线段都是向量,其起点和终点就是线段的起点

和终点。

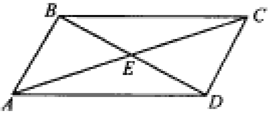


图 9.1.6

设平行四边形的对角线 AC 的中点为 E。只须证明 E 也是 BD 的中点或 $BE \parallel ED$, $|BE| = |ED|$ 或 $BE = -DE$ 或 $BE + DE = 0$ 即可。

$$BE + ED = BC + CE + DA + AE = (BC + DA) + (CE + AE)$$

由于 $ABCD$ 是平行四边形,故 $BC \parallel AD$,且 $|BC| = |AD|$,因此 $DA = -AD = -BC$,故 $BC + DA = 0$。又根据假设,E 是 AC 的中点,因此 $AE = EC = -CE$,由此又得 $CE + AE = 0$。因此

$$BE + DE = (BC + DA) + (CE + AE) = 0$$

这就证明了 E 也是 BD 的中点。

习题 9.1

1. 证明:恒等式 $|\alpha + \beta|^2 + |\alpha - \beta|^2 = 2(|\alpha|^2 + |\beta|^2)$。

2. 设 α, β, γ 都是复数,证明:$|\sqrt{\alpha^2 + \beta^2 + \gamma^2}| \leqslant \max\{|\alpha| + |\beta|, |\beta| + |\gamma|, |\gamma| + |\alpha|\}$。

3. 求证:当 $|\alpha| = 1$ 或 $|\beta| = 1$,但是 $\alpha \neq \beta$ 时,成立 $\left|\dfrac{\alpha - \beta}{1 - \bar{\alpha}\beta}\right| = 1$。

4. 计算:$\dfrac{(1 + i)^n}{(1 - i)^{n-2}}$。

5. 证明:如果 $|z| < \dfrac{1}{2}$,则 $|(1 + i)z^3 + iz| < \dfrac{3}{4}$。

6. 在复数平面上,以原点 O 为圆心作单位圆。设 z 是单位圆外一点,过 z 作圆的切线,设切点为 T。过 T 引 Oz 的垂线,设此垂线 Oz 与交于点 z_1,那么点 z_1 称为点 z 关于单位圆周的反演点,证明:$z_1 = \dfrac{1}{\bar{z}}$。

7. 解方程:$|x| - x = 1 + 2i$。

8. 设 3 个复数 z_1, z_2, z_3 满足条件 $|z_1| = |z_2| = |z_3| = 1, z_1 + z_2 + z_3 = 0$,证明:他们是一个正三角形的三个顶点。

9. 设 $\omega = -\dfrac{1}{2} + \dfrac{\sqrt{3}}{2}i$, a, b, c 代表三角形的三个顶点,证明:a, b, c 是逆时针绕行的正三角形的充分必要条件是 $a + b\omega + c\omega^2 = 0$。

10. 设 A, B, C, D 为平面上任意四点,证明:$AC \cdot BD \leqslant AB \cdot CD + AD \cdot BC$。

11. 设 $\omega = -\dfrac{1}{2} + \dfrac{\sqrt{3}}{2}i$,证明

$$(x + y + z)(x + \omega y + \omega^2 z)(x + \omega^2 y + \omega z) = x^3 + y^3 + z^3 - 3xyz$$

12. 证明:

(1) $\arctan\frac{2}{11}+\arctan\frac{24}{7}=\arctan\frac{1}{2}$；

(2) $\arccos\frac{2\sqrt{5}}{5}+\arcsin\frac{\sqrt{10}}{10}=\frac{\pi}{4}$；

(3) $\arctan n+\operatorname{arccot}(n+1)=\arctan(n^2+n+1)$。

13. 计算：$\arctan\frac{4}{3}+\arctan\frac{5}{12}+\arctan\frac{16}{63}$。

14. 从前有个富于冒险精神的年轻人，在他曾祖父的遗物中发现了一张羊皮纸，上面指出了一笔财富藏于何处。路线如下：

乘船至北纬________，西经________，即可找到一座荒岛。岛的北岸有一大片草地。草地上有一株橡树和一株松树。还有一座绞架，那是我们过去用来吊死叛变者的。从绞架走到橡树，并记住走了多少步；到了橡树向右拐个直角再走这么多步，在这里打个桩。然后回到绞架那里，朝松树走去，同时记住所走的步数；到了松树向左拐个直角再走这么多步。在这里也打个桩。在两个桩的正中挖掘，就可找到宝藏。(为了保密，这里已删去了文件中的经度和纬度)

曾祖父的的指示是够清楚的，于是这位年轻人就租了一条船前往。最后他找到了这座岛，也找到了橡树和松树。但使他大失所望的是绞架却不见了。因为经过长时间的风吹日晒雨淋，那座绞架早已腐烂，一点痕迹也没有了。

这一下年轻人陷入了绝望。他疯狂地在岛上乱挖起来。但是由于地方太大，所以一切都只是白费力气，最后只好两手空空十分扫兴地回家了。

其实，这位年轻人如果懂得点数学，特别是复数，他本来是可以找到宝藏的，现在请你来解答这笔宝藏藏于何处。

15. 一个人先向正东方向走了 r km，然后按逆时针方向与原来的方向偏转 θ 角，再向前走了 r km，然后按逆时针方向与原来的方向偏转 θ 角，再向前走了 r km…，问他向前走了 n 次后，离原来的出发点有多远。

16. 设 $\alpha_1=(a_1,b_1)$，$\alpha_2=(a_2,b_2)$ 表示平面中的向量，定义向量的加法法则为 $\alpha_1+\alpha_2=(a_1+a_2,b_1+b_2)$，并定义任意一个向量 $\alpha=(a,b)$ 的模为 $N(\alpha)=\sqrt{a^2+b^2}$。现假设在平面向量间定义了一种乘法 $*$ 满足以下性质：

(1) 全体平面向量在 $*$ 乘法下是自封的；

(2) $\alpha*\beta=\beta*\alpha$(乘法交换律)；

(3) $(\alpha*\beta)*\gamma=\alpha*(\beta*\gamma)$(乘法结合律)；

(4) $\alpha*(\beta+\gamma)=\alpha*\beta+\alpha*\gamma$，$(\alpha+\beta)*\gamma=\alpha*\gamma+\beta*\gamma$(乘法对于加法的分配率)；

(5) $(k,0)*(a,b)=(ka,kb)$；

(6) $N(\alpha*\beta)=N(\alpha)N(\beta)$(模与乘法的相容性)。

证明：

(1) 存在实数 u,v 使得 $(0,1)*(0,1)=(u,v)$；

(2) $(0,b)=(b,0)*(0,1)$；

(3) $(1,1)*(-1,1)=(u-1,v)$；

(4) $u=-1,v=0$；

(5) $(a_1,b_1)*(a_2,b_2)=(a_1a_2-b_1b_2,a_1b_2+a_2b_1)$。

17. 设 a,b 是平面上两个不共线的向量，那么如果 $\lambda a+\mu b=0$，则必有 $\lambda=0,\mu=0$，这里 λ,μ 是两个实数。

18. 设 M 把线段 AB 分成 $\lambda:\mu$ 的比例，O 是任意一点，$OA=a,OB=b$，用 a,b 来表出 OM。(这里的线段都是向量，其起点和终点就是线段的起点和终点)

19. 如图 9.1.7，在 $\triangle ABC$ 中，D 是 BC 的中点，E 是 AC 的中点。AD,BE 交于 G。

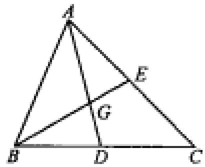


图 9.1.7

(1) 设 $BC=a,BA=b$。(以下的线段都是向量，其起点和终点就是线段的起点和终点) 用 a,b 表示 AC,AD 和 BE。

(2) 设 G 分 AD 为 $x:1$ 的比例，分 BE 为 $y:1$ 的比例，求 x,y。

(提示：利用 G 分 AD 为 $x:1$ 的假设，可用 AD 表出 AG，再利用(1) 的结果可用 a,b,x 表示 AG。另一方面，利用 14 题的结果和 G 分 BE 为 $y:1$ 的假设又可用 a,b,y 来表示 AG。由此再利用 13 题就可列出 x,y 的方程解出 x,y。)

(3) 证明：$GD=\frac{1}{3}AD,GE=\frac{1}{3}BE$。

(4) 设 $BD=\frac{1}{3}BC,CE=\frac{1}{3}CA$，证明：$GD=\frac{1}{7}AD,GE=\frac{1}{7}BE$。

9.2 复数的方根

虽然我们在 9.1 中已经复习了复数的运算，但是还有一个概念或"运算"还是值得单独拿出来复习一下。这就是复数的方根的概念。

定义 9.2.1 设 β 表示一个复数，如果复数 α 适合关系式 $\alpha^n=\beta$，则称 α 是 β 的一个 n 次方根。

定义了复数的方根的概念以后，首先发生的问题就是对于任意的复数 β 和正整数 n，是否总存在 β 的 n 次方根(因为对于实数来说，并不是任意一个实数都一定存在某个指定次数的方根的)？如果存在，又有几个？并且如何把它们计算出来？对这些问题的回答是：

定理 9.2.1 对于任意的复数 β 和正整数 n，总存在 β 的 n 次方根。一个不

等于 0 的复数的 n 次方根恰有 n 个。

证明　设 β 的三角表示为

$$\beta = r(\cos\theta + \mathrm{i}\sin\theta), r \geqslant 0, 0 \leqslant \theta < 2\pi$$

如果

$$\alpha = \rho(\cos\varphi + \mathrm{i}\sin\varphi), \rho \geqslant 0, 0 \leqslant \varphi < 2\pi$$

是 β 的 n 次方根的话，按照定义，就应该有

$$\alpha^n = \beta$$

或者

$$\alpha^n = (\rho(\cos\varphi + \mathrm{i}\sin\varphi))^n = \rho^n(\cos n\varphi + \mathrm{i}\sin n\varphi) = r(\cos\theta + \mathrm{i}\sin\theta) = \beta$$

由此得到

$$\rho^n = r, n\varphi = \theta + 2k\pi, \text{其中 } k \text{ 是任意整数}$$

由此得出

$$\rho = \sqrt[n]{r}, \varphi = \frac{\theta + 2k\pi}{n}, k = 0, \pm 1, \pm 2, \cdots$$

当 k 取不同的整数时，我们就得到 β 的所有可能的 n 次方根的表达式如下

$$\alpha_k = \sqrt[n]{r}, \left(\cos\frac{\theta + 2k\pi}{n} + \mathrm{i}\sin\frac{\theta + 2k\pi}{n}\right), k = 0, \pm 1, \pm 2, \cdots$$

因此 β 的 n 次方根的存在性是没有问题的。现在的问题是 β 能有多少个不同 n 的次方根呢？这时要注意，上面公式中的 k 虽然可以取无穷多个整数值，但这并不表示 β 有无穷多个不同的 n 次方根。因为当 k 取不同的整数值时，我们可能得到相同的 α_k。由于每当 k 增加或减少 1 时，α_k 的辐角就相应地增加或减少 $\frac{2\pi}{n}$，而一个圆周角的值为 2π，用除法可以算出一个圆周角共包含 $\frac{2\pi}{\frac{2\pi}{n}} = n$ 个 $\frac{2\pi}{n}$ 角，所以每当增加或较少 n 时，α_k 的值就会产生重复循环。所以我们只能得到 n 个不同的 n 次根

$$\alpha_0, \alpha_1, \cdots, \alpha_{n-1}$$

而其余的 α_k 一定和上面的这 n 个不同的 n 次根中的某一个相等。至于 α_k 究竟与上面的 n 个根中的哪一个相等，则可用带余数除法来决定。

设 $k = qn + h, 0 \leqslant h < n$，那么

$$\alpha_k = \sqrt[n]{r}\left(\cos\frac{\theta + 2k\pi}{n} + \mathrm{i}\sin\frac{\theta + 2k\pi}{n}\right) =$$

$$\sqrt[n]{r}\left(\cos\frac{\theta + 2(qn + h)\pi}{n} + \mathrm{i}\sin\frac{\theta + 2(qn + h)\pi}{n}\right) =$$

$$\sqrt[n]{r}\left(\cos\left(\frac{\theta + 2h\pi}{n} + 2q\pi\right) + \mathrm{i}\sin\left(\frac{\theta + 2h\pi}{n} + 2q\pi\right)\right) =$$

$$\sqrt[n]{r}\left(\cos\frac{\theta+2h\pi}{n}+\mathrm{i}\sin\frac{\theta+2h\pi}{n}\right)=\alpha_h$$

因此,我们就证明了:每一个复数 $\beta\neq0$,都恰有 n 个不同的 n 次方根。

设 $\beta\neq0$,那么根据 β 的 n 个不同的 n 次方根的表达式和复数的几何意义就可看出,这 n 个 n 次方根都分布在同一个半径为 $\sqrt[n]{r}=\sqrt[n]{|\beta|}$ 的圆上,并且构成一个正 n 边形的 n 个顶点。图 9.2.1 中画出了 1 的 8 个 8 次方根。图 9.2.1 中所示的方根给出了一种特别的情况,即

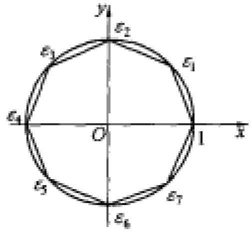


图 9.2.1

定义 9.2.2 1 的任何一个 n 次方根称为 n 次单位根。

由于 1 的辐角是 0,所以在复数的方根的一般表达式中(见定理 9.2.1) 令 $\theta=0$ 就得到 n 个 n 次单位根的表达式如下

$$\varepsilon_k=\cos\frac{2k\pi}{n}+\mathrm{i}\sin\frac{2k\pi}{n},k=0,1,\cdots,n-1$$

这些根都分布在以原点为圆心的单位圆周上,并且把它 n 等分。1是其中的一个分点,当 n 是偶数时,-1 也是一个分点,当 n 是奇数时,-1 就不是分点了。除了 ±1 外,其余的 n 次单位根都不是实数,因而都不在实轴上,这些不在实轴上的 n 次单位根对于实轴是对称的,也就是说,不在实轴上的 n 次单位根是两两共轭的。

用 n 次单位根可以表出任意复数的 n 次方根。设 α 是复数 β 的任一个 n 次方根,那么

$$\alpha=\alpha\varepsilon_0,\alpha\varepsilon_1,\cdots,\alpha\varepsilon_{n-1}$$

显然是 n 个两两不同的复数。而且由于 $(\alpha\varepsilon_k)^n=\alpha_n\varepsilon_k^n=\beta$,所以他们又都是 β 的 n 次方根,因而恰好是 β 的 n 个 n 次方根。单位根有以下性质:

定理 9.2.2

(1) 两个 n 次单位根的乘积还是一个 n 次单位根;

(2) 一个 n 次单位根的倒数还是 n 次单位根;

(3) 两个 n 次单位根的商还是一个 n 次单位根;

(4) 一个 n 次单位根的共轭还是 n 次单位根;

(5) $(\varepsilon_k)^l=(\varepsilon_l)^k$;

(6) $\varepsilon_k = \varepsilon_l$ 的充分必要条件是 $k - l \equiv 0 \pmod n$ 或 k 和 l 相差一个 n 的倍数；

(7) 当 m 不是 n 的倍数时，$1 + \varepsilon_1^m + \varepsilon_2^m + \cdots + \varepsilon_{n-1}^m = 0$；

(8) $1 + \varepsilon_1 + \varepsilon_2 + \cdots + \varepsilon_{n-1} = 0$；

(9) 设 $\varepsilon_k \neq 0$，则 $1 + \varepsilon_k + (\varepsilon_k)^2 + \cdots + (\varepsilon_k)^{n-1} = 0$。

证明　由 n 次单位根的表达式 $\varepsilon_k = \cos\dfrac{2k\pi}{n} + \mathrm{i}\sin\dfrac{2k\pi}{n}$ 可以看出

$$\varepsilon_k\varepsilon_l = \varepsilon_{k+l}, \varepsilon_k^{-1} = \varepsilon_{-k}, \frac{\varepsilon_k}{\varepsilon_l} = \varepsilon_k\varepsilon_l^{-1} = \varepsilon_k\varepsilon_{-l} = \varepsilon_{k-l}$$

这就证明了(1)、(2)、(3)。

又

$$\overline{\varepsilon_k} = \frac{\varepsilon_k\overline{\varepsilon_k}}{\varepsilon_k} = \frac{|\varepsilon_k|}{\varepsilon_k} = \frac{1}{\varepsilon_k} = \varepsilon_{-k}, (\varepsilon_k)^l = \varepsilon_{kl} = (\varepsilon_l)^k$$

这就证明了(4)、(5)。

(6) 在定理9.2.1的证明中已经证明了 $\varepsilon_k = \varepsilon_h, 0 \leqslant h \leqslant n-1$ 的充分必要条件是

$$k = qn + h, 0 \leqslant h \leqslant n-1$$

因此 $\varepsilon_k = \varepsilon_l$ 的充分必要条件是存在 $0 \leqslant h \leqslant n-1$ 使得

$$k = q_1n + h, l = q_2n + h$$

由此易得 $k - l \equiv 0 \pmod n$。反之如果 $k - l \equiv 0 \pmod n$，又设 $k = q_1n + h$，$0 \leqslant h \leqslant n-1$，那么显然就有 $l = q_2n + h$，因而 $\varepsilon_k = \varepsilon_l$。这就证明了(6)。

(7) 当 m 不是 n 的倍数时，$\varepsilon_1^m = \varepsilon_m \neq 1$，故

$$\begin{aligned}1 + \varepsilon_1^m + \varepsilon_2^m + \cdots + \varepsilon_{n-1}^m &= 1 + \varepsilon_1^m + (\varepsilon_1^2)^m + \cdots + (\varepsilon_1^{n-1})^m = \\ &1 + \varepsilon_1^m + (\varepsilon_1^m)^2 + \cdots + (\varepsilon_1^m)^{n-1} = \\ &\frac{1 - (\varepsilon_1^m)^n}{1 - \varepsilon_1^m} = \frac{1 - (\varepsilon_1^n)^m}{1 - \varepsilon_1^m} = \frac{1 - 1}{1 - \varepsilon_1^m} = 0\end{aligned}$$

在(7)中令 $m = 1$ 就得到(8)，在(7)中令 $m = k$ 就得到(9)。

由定理9.2.2可以看出 ε_1 这个 n 次单位根有一个特别好的性质，那就是

$$\varepsilon_k = \varepsilon_1\varepsilon_1\cdots\varepsilon_1 = \varepsilon_1^k, k = 0,1,\cdots,n-1$$

因此1的 n 个 n 次单位根就可以写成 $1 = \varepsilon_1^0, \varepsilon_1, \varepsilon_1^2, \cdots, \varepsilon_1^{n-1}$，这是一种多么好的表达式啊！那么，是不是所有的 n 次单位根都具有这种性质呢？答案是否定的。因此有必要单独抽出一种新的概念来，即：

定义 9.2.3　设 ε 是一个 n 次单位根，如果

$$1, \varepsilon, \varepsilon^2, \cdots, \varepsilon^{n-1}$$

恰好是1的 n 个 n 次单位根，则称 ε 是一个 n 次单位原根。

下面的定理给出了一个 n 次单位根是否是 n 次单位原根的判别条件，利用它就可得到所有的 n 次单位原根。

定理9.2.3 $\varepsilon=\varepsilon_k$ 是一个 n 次单位原根的充分必要条件是 $(k,n)=1$，即 k 与 n 是互素的整数。

证明 必要性：设 $\varepsilon=\varepsilon_k$ 是一个 n 次单位原根，那么按照 n 次单位原根的定义可知，必存在某一个整数 $0\leqslant m\leqslant n-1$，使得 $(\varepsilon_k)^m=\varepsilon_1$，由定理9.2.2知这就是 $\varepsilon_{km}=\varepsilon_1$，或者

$$\varepsilon_{km}=\cos\frac{2km\pi}{n}+\mathrm{i}\sin\frac{2km\pi}{n}=\cos\frac{2\pi}{n}+\mathrm{i}\sin\frac{2\pi}{n}=\varepsilon_1$$

由此可知

$$\frac{2km\pi}{n}=\frac{2\pi}{n}+2q\pi,\text{其中 } q \text{ 是一个整数}$$

由此得出 $km-qn=1$，因而 $(k,n)\mid km-qn=1$，故必有 $(k,n)=1$。

充分性：设 k 与 n 互素，则 $1,\varepsilon_k,\varepsilon_k^2,\cdots,\varepsilon_k^{n-1}$ 必是两两不同的。否则假设有 $0\leqslant m_1<m_2\leqslant n-1$，使得 $\varepsilon_k^{m_1}=\varepsilon_k^{m_2}$ 或者 $\varepsilon_{km_1}=\varepsilon_{km_2}$。那么比较 $\varepsilon_{km_1}=\varepsilon_{km_2}$ 两边的辐角可知

$$\frac{2km_1\pi}{n}=\frac{2km_2\pi}{n}+2q\pi,\text{其中 } q \text{ 是一个整数}$$

由此得出

$$k(m_1-m_2)=qn$$

故 $n\mid k(m_1-m_2)$，由于 $(k,n)=1$，因此 $n\nmid k$，这就得出必有 $n\mid(m_1-m_2)$，故 $|m_1-m_2|\geqslant n$，但是由于 $0\leqslant m_1<m_2\leqslant n-1$，所以又有 $|m_1-m_2|<n$。这是一个矛盾，所得的矛盾就说明了 $1,\varepsilon_k,\varepsilon_k^2,\cdots,\varepsilon_k^{n-1}$ 必是两两不同的。按照定义，这就意味着 $\varepsilon=\varepsilon_k$ 是一个 n 次单位原根。

1的3次单位根是一个经常要用到的符号，不难算出1的3个3次单位根是

$$1,\ -\frac{1}{2}+\frac{\sqrt{3}}{2}\mathrm{i}\text{ 和 }-\frac{1}{2}-\frac{\sqrt{3}}{2}\mathrm{i}$$

习惯上，一般记 $\omega=-\frac{1}{2}+\frac{\sqrt{3}}{2}i$，因此 $\omega^2=-\frac{1}{2}-\frac{\sqrt{3}}{2}\mathrm{i}$。它们满足关系

$$1+\omega+\omega^2=0$$

$$(\omega)^2=\omega^2,(\omega^2)^2=\omega,\overline{\omega}=\omega^2,\overline{\omega^2}=\omega$$

当 n 是3的倍数时，$1^n+\omega^n+(\omega^2)^n=3$，当 n 不是3的倍数时，$1^n+\omega^n+(\omega^2)^n=0$。

习题9.2

1. 计算下列方根

(1) $\sqrt[3]{\mathrm{i}}$ (2) $\sqrt[4]{-4}$ (3) $\sqrt[6]{-27}$

2. 计算

(1) $\sqrt[6]{\dfrac{1-\mathrm{i}}{\sqrt{3}+\mathrm{i}}}$　　　(2) $\sqrt[8]{\dfrac{1+\mathrm{i}}{\sqrt{3}-\mathrm{i}}}$

3. 证明：如果 $z+\dfrac{1}{z}=2\cos\theta$，则 $z^n+\dfrac{1}{z^n}=2\cos n\theta$。

4. 求所有满足条件 $\overline{x}=x^{n-1}(n>1)$ 的复数。

5. 解方程：$(x+1)^n-(x-1)^n=0$。

6. 设 ε 是一个 $2n$ 次单位原根，计算：$1+\varepsilon+\varepsilon^2+\cdots+\varepsilon^{n-1}$。

7. 设 ε 是一个 n 次单位根，计算：$1+2\varepsilon+3\varepsilon^2+\cdots+n\varepsilon^{n-1}$。

8. 设 $\omega=-\dfrac{1}{2}+\dfrac{\sqrt{3}}{2}\mathrm{i}$，证明：

(1) 当 n 是 3 的倍数时，$1^n+\omega^n+(\omega^2)^n=3$，
当 n 不是 3 的倍数时，$1^n+\omega^n+(\omega^2)^n=0$；

(2) 求 $1+C_n^3+C_n^6+\cdots+C_n^{3k-3}+C_n^{3k}$，$k=\left[\dfrac{n}{3}\right]$。

9.3　群、环和域

在上一节中，我们引入了单位根的概念，n 次单位根的全体作为一个集合，已经表现出一些一般的性质，这些性质如果不特别点出，光局限于单位根这个概念的本身，可能不被注意到，但是一旦把这些性质抽象为更一般的概念，再回过头需看向单位根的集合这样的具体对象，就会感到格外清晰。用这样的方式去看后面的一些内容时也是如此。因此，在本节中，我们将先引进一些近世代数中的基本概念。

首先我们要比较确切地说明运算的含义。虽然这一概念我们从小学起就开始接触，但却不一定认真思考过它的确切意义。

定义 9.3.1　设 A,B 是任意两个集合，那么全体有序的元素对 (a,b)，$a\in A$，$b\in B$ 的集合 $\{(a,b)\mid a\in A,b\in B\}$ 称为 A,B 的乘积集合，记为 $A\times B$。

定义 9.3.2　设 A 是一个非空集合，那么一个 A 中的代数运算意为一个从集合 $A\times A$ 到 A 的映射。

例如通常实数的加法就是映射 $(x,y)\to x+y$，乘法就是映射 $(x,y)\to xy$。当所考虑的集合就是全体实数 $\mathbf{R}$ 时，从 $\mathbf{R}\times\mathbf{R}$ 到 $\mathbf{R}$ 的映射实际上就是大学数学分析中的所谓二元函数 $f(x,y)$，显然 $x+y$ 和 xy 都是特殊的二元函数。

定义 9.3.3　如果对非空的集合 G 中的元素可以定义一个称为乘法或加法的运算，且此运算满足以下性质，则称集合 G 是一个群。

(1) 封闭性。如果 $a \in G, b \in G$,那么 $ab \in G$。

(2) 结合律。对 G 中任意元素 a,b,c 成立 $a(bc)=(ab)c$。

(3) 单位元的存在性。在 G 中存在一个称为单位元的元素 e,它具有性质:对 G 中任意元素 a 都成立 $ea = ae = a$。

(4) 逆元的存在性。对 G 中任意元素 a,存在一个称为 a 的逆元的元素 a^{-1},它具有性质:$aa^{-1} = a^{-1}a = e$。

当群中的运算称为加法时,定义 9.3.3 中的条件(2) ~ (4) 就成为

(2) 结合律。对 G 中任意元素 a,b,c 成立 $a+(b+c)=(a+b)+c$。

(3) 单位元的存在性。在 G 中存在一个称为单位元的元素 0,它具有性质:对 G 中任意元素 a 都成立 $0+a=a+0=a$。

(4) 逆元的存在性。对 G 中任意元素 a,存在一个称为 a 的逆元的元素 $-a$,使得 $a+(-a)=(-a)+a=0$。

另外,在运算的定义中,已含有了封闭性的要求,但是为了强调群的定义中对运算封闭性的要求,我们还是把它作为一个条件明确提出来以引起注意。

下面来看几个例子:

例 9.3.1 全体整数 **Z** 对于加法构成一个群,同样全体有理数 **Q**,全体实数 **R**,全体复数 **C** 对于加法也构成一个群。

例 9.3.2 全体非零的实数 $\mathbf{R}_*$,全体正实数 $\mathbf{R}^+$ 对于乘法也构成一个群。

例 9.3.3 设 n 是一个正整数,那么全体 n 次单位根对于复数的乘法构成一个群,这个群有一个特别的记号 U_n。特别 $U_2 = \{1,-1\}$ 是仅有两个元素,而且都是实数组成的集合,这是 U_n 中唯一一个具有这种性质的集合。

例 9.3.4 设 F 是平面上的一个图形。考虑 F 在空间中的所有运动,这些运动可以看成是对 F 所作的变换。设 G_F 表示所有使 F 保持不动的运动所造成的变换。显然,在 G_F 中变换的乘法是封闭的,满足结合律;G_F 中存在单位元,就是恒等变换;且 G_F 中每个变换的逆变换仍在 G_F 中。因此 G_F 构成一个群。这个群通常称为图形 F 的对称群,它反映了图形 F 的对称性质。

例如,设 F 是平面上的一个正方形,如图 9.3.1 所示。

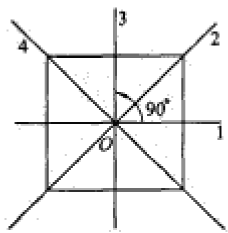


图 9.3.1

那么可以看出保持正方形不变的运动有:绕点 O 做 90°,180°,270°,360° 的旋转和对直线 1,2,3,4 的镜面反射。因此 G_F 由 8 个元素组成。如果用 T 代表绕点 O 90° 的旋转,用 R 代表对直线 1 的镜面反射,那么利用变换的乘法,就可以把 G_F 的 8 个元素用 T,R 表示出来。

$$G_F = \{T, T^2, T^3, T^4, R, RT, RT^2, RT^3\}$$

其中，T^4 就是恒等变换，也就是 G_F 的单位元。T,R 称为 G_F 的生成元。所以 G_F 是一个只有两个生成元的 8 元群。

为了看下一个例子，我们首先引进几个概念：

定义9.3.4 集合$\{1,2,\cdots,n\}$到自身的一个1—1映射称为一个 n 元置换。通常记为

$$\tau=\begin{pmatrix}1, & 2 & ,\cdots, & n\\ \tau(1), & \tau(2) & ,\cdots, & \tau(n)\end{pmatrix}$$

定义9.3.5 如果一个 n 元置换σ将$1,2,\cdots,n$中某m个数$\alpha_1,\alpha_2,\cdots,\alpha_m$轮换，即

$$\sigma(\alpha_1)=\alpha_2,\sigma(\alpha_2)=\alpha_3,\cdots,\sigma(\alpha_{m-1})=\alpha_m,\sigma(\alpha_m)=\alpha_1$$

而保持其余各个数不变，则称 σ 为一个轮换，记为

$$\sigma=(\alpha_1\alpha_2\cdots\alpha_m)$$

特别，当 $m=2$ 时，σ 称为对换。

定义9.3.6 如果轮换 σ_1 和 σ_2 没有相同的元素，则称 σ_1 和 σ_2 是不相交的轮换。

例9.3.5 设所有的 n 元置换组成的集合为S_n，那么可以看出 S_n 中变换的乘积是封闭的，结合的。S_n 中有单位元，就是恒同变换，又设

$$\tau=\begin{pmatrix}1, & 2 & ,\cdots, & n\\ \tau(1), & \tau(2) & ,\cdots, & \tau(n)\end{pmatrix}$$

是 S_n 中任一元素，那么显然 S_n 中的元素

$$\tau=\begin{pmatrix}\tau(1), & \tau(2) & ,\cdots, & \tau(n)\\ 1, & 2 & ,\cdots, & n\end{pmatrix}$$

就是 τ 的逆元，因此 S_n 中每一个变换存在逆元，这就说明 S_n 构成一个群，称为 n 元置换群。

由于 n 元置换群是一个很重要也很典型的可以看得见摸得着的群，因此我们给出它的一些重要性质如下：

定理9.3.1 设 S_n 表示 n 元置换群，那么

(1) S_n 共有 $n!$ 个元素；

(2) 任何一个置换都能表示成为一些不相交的轮换的乘积。

证明 (1) 既然置换是一个 1—1 的变换，所以对任何置换 τ 来说

$$\tau(1)\tau(2)\cdots\tau(n)$$

都是$\{1,2,\cdots,n\}$ 的一个排列。因此 S_n 共有 $n!$ 个元素。

(2) 设 τ 表示任一置换，h 是在 τ 下保持不变的数的个数。我们对 $n-h$ 作数学归纳法。

当 $n-h=0$ 时，τ 就是单位置换 I，显然 $I=(1)(2)\cdots(n)$ 是 n 个不相交

的轮换的乘积，故(2)的结论成立。

假设当 $n-h<k$ 时，结论成立。那么当 $n-h=k$ 时，根据 h 的定义可知，有 k 个元素在 τ 的作用下要变成和它自身不同的元素。任取其中一个，比如说 α_1，考虑叙列

$$\alpha_1,\tau(\alpha_1),\tau^2(\alpha_1),\cdots$$

那么因为 n 是一个有限数，所以上述叙列中必有重复出现的数。设 $\tau^t(\alpha_1)$ 是第一个这样的数。于是根据 $\tau^t(\alpha_1)$ 的意义，必有

$$\tau^t(\alpha_1)=\tau^s(\alpha_1),s<t$$

如果 $s\geqslant 1$，那么根据 τ 是1—1的即得

$$\tau^{t-1}(\alpha_1)=\tau^{s-1}(\alpha_1),s<t$$

(否则用 τ 对 $\tau^{t-1}(\alpha_1)$ 和 $\tau^{s-1}(\alpha_1)$ 各作用一次将得出矛盾)。而这与 $\tau^t(\alpha_1)$ 是第一个与前面重复的数的定义相矛盾，因此不可能。故必须有 $\tau^t(\alpha_1)=\alpha_1$。设

$$\tau(\alpha_1)=\alpha_2,\tau(\alpha_2)=\alpha_3,\cdots,\tau(\alpha_{t-1})=\alpha_t$$

于是
$$\tau(\alpha_t)=\tau^t(\alpha_1)=\alpha_1$$

这就说明 τ 与轮换 $\sigma=(\alpha_1\alpha_2\cdots\alpha_t)$ 对 $\alpha_1,\alpha_2,\cdots,\alpha_t$ 这 t 个数的作用是相同的。显然，对于置换 $\tau\sigma^{-1}$ 来说保持不变的数的个数比 τ 增加了 t 个，因而 $n-h$ 减少了 t 个，根据归纳法假设可知 $\tau\sigma^{-1}=\sigma_1\sigma_2\cdots\sigma_l$，其中 $\sigma_1,\sigma_2,\cdots,\sigma_l$ 是一些不相交的轮换，而且显然这些轮换与 σ 也是不相交的(否则将和 τ 是1—1的变换相矛盾)，因此

$$\tau=\sigma_1\sigma_2\cdots\sigma_l\sigma$$

已表示成一些不相交的轮换的乘积，故对 $n-h=k$ 的情况结论也成立。因此由数学归纳法就证明了(2)的结论。

唯一性也可以用数学归纳法证明。

从群的定义和上面的例子可以看出，群是一种几乎简单得不能再简单的代数结构，然而它又能包含相当广泛的内容。这就决定了群和数一样可以得到很广泛的应用，而且就是这么一个初看起来很简单的结构实际上却可以发展出很丰富的理论，例如子群、有限群、交换群等等。

在群的定义里并没有包含运算的交换性，却要求运算的结合性。由此看来，结合性是比交换性更基础的性质。

定义9.3.7 如果群 G 中的运算是可交换的，即对任意 $a\in G,b\in G$ 都成立

$$ab=ba$$

那么 G 就称为交换群或阿贝尔群。交换群的运算常用加法表示。

定义9.3.8 如果群 G 的元素个数是有限的，G 就称为有限群，否则称为

无限群。有限群所含元素的个数称为群的阶，记为$[G:1]$。

定义 9.3.9 群 G 中所有与 G 中任意元素都能交换的元素组成的集合称为 G 的中心，记为 $C(G)$。

可以证明(见习题 9.3) 任何一个群的中心本身也构成一个群，这就很有意思。像中心这种概念，把它提出来本身就已经是抓住了群的某种特性。在代数中，概念起了很重要的作用。在提出某种概念之前，如果后来表明这一概念是很有用的，那就表明，研究者已经注意到了研究对象的某种值得注意的性质，概念的提出是研究者拥有了一种新的观察角度。在数学的大多数领域，我们经常离不开公式的推导以及计算。但是在有些领域，你几乎见不到多少式子，而是从一开始就会遇到一连串的概念，依靠这些概念和推理，最后也能得出许多很深刻的结果。

下面我们来看一下群有什么一般的性质。

定理 9.3.2 设 G 是一个群，那么

(1) 对任意 $a\in G, b\in G$，方程 $ax=b$ 和 $ya=b$ 有解；

(2) 成立消去律，即由 $ax=ay$ 以及 $xa=ya$ 可以得出 $x=y$；

(3) 群中的元素相乘时可以任意结合；特别 $a\cdot a\cdot\cdots\cdot a$($n$ 个) 和相乘的结合方式无关，因此记号 a^n 是有意义的，如果定义 $a^0=e, a^{-n}=(a^{-1})^n(n>0)$，那么对于任意整数都成立

$$a^m\cdot a^n=a^{m+n},(a^m)^n=a^{mn}$$

如果群中的运算用加法表示，那么上面的指数律就成为

$$ma+na=(m+n)a, m(na)=(mn)a$$

(4) 如果 G 是交换群，那么 G 中运算的交换性对任意多个元素的乘积也成立，既可以任意方式将相邻的两项乘积交换。

证明 (1) 由 $a(a^{-1}b)=(aa^{-1})b=eb=b$ 和 $(ba^{-1})a=b(a^{-1}a)=be=b$ 即可知(1) 的结论成立。

(2) 设 $ax=ay$，那么在此式两边用 a^{-1} 左乘，即可得出 $x=y$，同理可证右边的消去律成立。

(3) 设 n 是任意自然数，$a_1,a_2,\cdots,a_n$ 是群中的元素。对命题：群中 k 个元素可以任意结合 k 做第二数学归纳法可证 $a_1,a_2,\cdots,a_n$ 在任意的结合下相乘所得的乘积都等于

$$a_1a_2\cdots a_n$$

就可证明(3)。所谓第二数学归纳法就是不仅假设当自然数等于 k 时命题成立，由此推出命题 $k+1$ 对也成立；而是假设对一切小于或等于 k 的自然数命题成立，在此前提下推出命题对 $k+1$ 也成立。可以证明普通的数学归纳法和第二数学归纳法是等价的。

(4) 与(3) 类似可用数学归纳法证明。

群的一个子集也可能本身仍构成一个群，这时我们称这个子集为群的子群。

定义 9.3.10 如果群 G 的非空子集 H 对于群 G 的运算也构成一个群，则称 H 为 G 的子群。

在这个定义中，值得注意的一点是 H 中的运算必须和 G 中的运算相一致，也就是说，如果在 H 中定义了另一种与 G 中不同的运算，而且即使 H 在这种运算下也构成群，H 也不能称为 G 的子群。这时你只能把 H 看成与 G 毫无关系的另一个群。

紧接着这个定义发生的问题是 G 的非空子集 H 要适合什么条件才能成为 G 的子群呢?

首先，如果 H 包含元素 a,b，那么它也必须包含 ab，否则 H 中的运算就不封闭了(再次强调 H 中的运算继承了 G 中的运算)。另外 H 必须有单位元 e'，由 $e'e' = e' = ee'$ 及群的消去律可知 $e' = e$。换句话说，单位元 e 也必须属于 H，最后 H 要能够成群，还必须包含它本身元素的逆元，由此就得出 H 是 G 的子群的 3 个必要条件，可以证明，这 3 个条件也是充分的。这就是

定理 9.3.3 群 G 的子集 H 是 G 的子群的充分必要条件是:

(1) $a \in H, b \in H$ 蕴含 $ab \in H$;

(2) $e \in H$;

(3) $a \in H$ 蕴含 $a^{-1} \in H$。

证明 条件的必要性上面已经证明，这些条件的充分性是显然的。

定理 9.3.4 任意个子群的交还是子群。

证明 由定理 9.3.3 知，任意子群都包含单位元，因此任意子群的交都不空且包含单位元。又设 a,b 属于它们的交，那么 a,b 就属于每一个子群，因此由定理 9.3.3 可知 ab 和 a^{-1} 也属于每一个子群，因而属于它们的交。再由定理 9.3.3 就得出任意个子群的交还是子群。

设 M 是 G 的非空子集，考虑所有包含 M 的 G 的子群，这种子群不可能组成空集，因为 G 本身就是一个这样的子群。根据定理 9.3.4 所有这种子群的交仍然是一个包含 M 的子群，并且是包含 M 的最小子群。

定义 9.3.11 设 M 是 G 的非空子集，称所有包含 M 的 G 的子群的交是由 M 生成的子群，记为(M)。

定理 9.3.5 设 $span\ M$ 是由 M 中的元素以及它们的逆所得出的所有可能的乘积组成的集合，则

$$span\ M = (M)$$

证明 容易由定义证明

$$span\ M \subset (M) \subset span\ M$$

因此
$$span\ M = (M)$$

定义 9.3.12 设 M 是 G 的非空子集,如果$(M) = G$,则称 M 是 G 的一组生成元。如果 M 是有限集,那么 G 就称为是有限生成的。

下面考虑一种最简单的群,即

定义 9.3.13 由一个元素生成的群称为循环群。

定理 9.3.6

(1) 设 G 是循环群,那么必存在 $a \in G$,使得 G 中任意一个元素都可写成 a^n 的形式,其中 n 是一个整数。

(2) 循环群一定是交换的。

(3) 循环群的子群仍是循环群。

证明 (1) 由循环群的定义即得。

(2) 由(1)的结论和定理9.3.2(3)中的指数律即知 G 中任意两个元素可写成 a^m 和 a^n,而 $a^m \cdot a^n = a^{m+n} = a^n \cdot a^m$,因而是可交换的。

(3) 设 G 是循环群,H 是 G 的子群。当 $H = \{e\}$ 时,结论显然。以下设 $H \neq \{e\}$,因此必有不是单位元的元素 a 使得 $G = (a)$。因而 G 中的元素从而 H 中的元素都具有 a^n 的形式。由于如果 $a^n \in H$,那么必有$(a^n)^{-1} = a^{-n} \in H$,而 n 和 $-n$ 二者之中必有一个是正整数,因此 H 中必含有 a 的正整数方幂 a^n。由自然数的最小数原理。可设 k 是使得 $a^n \in H$ 的最小正整数。

任取 H 中元素 a^n。设 $n = qk + r, 0 \leqslant r < k$,于是

$$a^r = a^{n-qk} = a^n \cdot (a^k)^{-q} \in H$$

而由 k 的最小性的定义就可得出 r 必须是0,因此 $n = qk$,故 H 中任意元素都是 a^k 的方幂,即 $H = (a^k)$。这就证明了 H 仍是循环群。

有些群表面上看起来具体的元素和运算都不相同,但是其实它们的结构是相同的,这时我们可把它们看成本质上相同的群。

定义 9.3.14 设 G_1 和 G_2 是两个群。如果存在 G_1 和 G_2 之间的1—1映射 σ 使得对于所有的 $x \in G_1, y \in G_1$ 都有

$$\sigma(xy) = \sigma(x)\sigma(y)$$

那么就称 G_1 同构于 G_2,记为 $G_1 \cong G_2$。

称 σ 是 G_1 和 G_2 之间的同构映射。

注意在同构的定义中 xy 中间的乘法是 G_1 中的运算,$\sigma(x)$ 和 $\sigma(y)$ 之间的运算是 G_2 中的运算,在定义中这两种运算都写成乘法,但是在具体的例子当中,这些运算可能用其他符号表示。

容易证明群之间的同构是一种等价关系。

定理 9.3.7 任何一个循环群或同构于整数加群或同构于某个正整数

m 的剩余类组成的加群。

证明 设 $G=(a)$ 是循环群，Z 是整数加群。如果 G 是无限的，那么 $G=\{a^n \mid n=0,\pm1,\pm2,\cdots\}$，令 $\sigma(a^n)=n$，那么易证 σ 是 G 和 Z 之间的 1—1 对应，且

$$\sigma(a^m\cdot a^n)=\sigma(a^{m+n})=m+n=\sigma(a^m)+\sigma(a^n)$$

因此 σ 是 G 和 Z 之间的同构，而 $G\cong Z$。

如果 G 是有限的。那么 $a,a^2,a^3,\cdots,a^i,\cdots$ 中必有重复者，因而存在一个正整数 n，使得 $a^n=e$。设 m 是使得 $a^n=e$ 成立的最小的非负整数，称为 a 的阶。那么 $a^m=e$。且仿照定理 9.3.6(3) 中的方法易证当且仅当 $h\equiv k(\mathrm{mod}\ m)$ 时，成立 $a^h=a^m$，因此 $\sigma(a^n)=n$ 是 G 与 m 的剩余类组成的加群 $Z(m)$ 之间的 1—1 对应。与无限循环群的情况相同，可证 σ 是 G 和 $Z(m)$ 之间的同构，因而 $G\cong Z(m)$。

由定理 9.3.7 的证明可知，如果 G 是一个有限群，那么对 G 中任意元素 a，都存在一个使得 $a^n=e$ 成立的最小的非负整数，这引出如下的定义。

定义 9.3.15 设 G 是任意一个群，a 是 G 中任意一个元素。如果对于 a，存在一个使得 $a^n=e$ 成立的最小的非负整数 k，就称 a 的阶为 k，否则就称 a 的阶是无穷大。

定理 9.3.8(拉格朗日定理) 设 G 是一个有限群，H 是 G 的子群，那么 H 的阶必是 G 的阶的因子。

拉格朗日 (Lagrange, Joseph Louis, 1736—1813)，法国数学家、力学家、天文学家，生于意大利的都灵，卒于法国巴黎。

证明 对 G 中任意两个元素 a,b 定义如果 $ba^{-1}\in H$，则称 a,b 对 H 左同余，记为

$$a\equiv b(\mathrm{mod}_l H)$$

换句话说，$a\equiv b(\mathrm{mod}_l H)$ 就等价于 $b=ha$，其中 h 是 H 中的某个元素。

同样可以定义右同余为 $b=ah$ 或者 $a^{-1}b\in H$，记为 $a\equiv b(\mathrm{mod}_r H)$。

容易证明左右同余都是一种等价关系。

因此用左同余或右同余可以把 G 中互相同余的元素分成一类，称为左同余类或右同余类。称与 a 左同余的所有元素组成的集合为 a 的左同余类或左陪集，记为 Ha。称与 a 右同余的所有元素组成的集合为 a 的右同余类或右陪集，记为 aH。

我们证明 $Ha=Hb$ 的充分必要条件是 $a\equiv b(\mathrm{mod}_l H)$。当时 $a\not\equiv b(\mathrm{mod}_l H)$ 时，$Ha\cap Hb=\varnothing$。

先证上面命题的前半部分。设 $Ha=Hb$，那么由于显然 $a\in Ha$，故 $a\in Hb$，因而 $a\equiv b(\mathrm{mod}_l H)$。

反之，如果 $a\equiv b(\mathrm{mod}_l H)$，设 $x\in Ha$，那么 $x\equiv a(\mathrm{mod}_l H)$，由于左同余是等价关系，因此 $x\equiv b(\mathrm{mod}_l H)$，因而 $x\in Hb$，这就说明 $Ha\subset Hb$，同理可证

$Hb \subset Ha$，因此 $Ha = Hb$。

现在证明上面命题的后半部分。设 $a \not\equiv b(\mathrm{mod}_l H)$，如果 $Ha \cap Hb \neq \varnothing$，那么存在 $c \in Ha \cap Hb$，因而由上面的证明可知 $a \equiv c \equiv b(\mathrm{mod}_l H)$，因而 $Ha = Hc = Hb$；这与 $Ha \cap Hb \neq \varnothing$ 矛盾，这就证明了上面命题的后半部分。

由上面的证明可知任意两个左陪集 Ha，Hb 或者重合，或者不相交。

下面我们再证明，所有的左陪集所包含的元素个数都是相同的。它们所包含的元素的个数就是 H 的阶。

首先证明 $Ha = \{ha \mid h \in H\}$。事实上，如果 $x \in Ha$，那么按照 Ha 的定义，就有 $x \equiv a(\mathrm{mod}_l H)$，因此 $x = ha$，因而 $Ha \subset \{ha \mid h \in H\}$；反之如果 $x \in \{ha \mid h \in H\}$，那么 $x = ha$，因而 $x \equiv a(\mathrm{mod}_l H)$，按照 Ha 的定义，就有 $x \in Ha$，这就说明 $\{ha \mid h \in H\} \subset Ha$。

现在考虑 H 与 Ha 之间的一个映射 $\varphi: h \to ha$。如果 $h = k \in H$，那么显然 $ha = ka \in Ha$，反之如果 $ha = ka \in Ha$，那么由群的消去律可知 $h = k \in H$。由此可知 $h = k \in H$ 的充分必要条件是 $ha = ka \in Ha$。这就说明 $\varphi: h \to ha$ 是 H 与 Ha 之间的一个 1—1 映射。因而 H 与 Ha 所含的元素个数一定是相同的，而且就等于 H 的阶。

由于 G 中任意一个元素 x 必定属于某一个左陪集(至少它属于 Hx)，所以我们可以把 G 分解成为两两互不相交的左陪集的并

$$G = \bigcup_{a \in G} Ha$$

(并号下面的脚标取得使得参与并的元素两两互不同余)，由于 G 是有限集，所以上式并号中的左陪集的个数也是有限的，设共有 k 个，那么分别计算上式两边的元素个数就得到

$$[G:1] = k[H:1]$$

这就证明了 $[H:1] \mid [G:1]$，即子群的阶一定是有限群的阶的因子。上式中的 k 就称为子群 H 在 G 中的指数，记为 $[G:H]$。由此得到指数公式

$$[G:H] = \frac{[G:1]}{[H:1]}$$

它说明，H 的左陪集的指数就是 k，同理可证 H 的右陪集的指数就是 k。因此我们又得到 H 的左陪集和右陪集的数目是相等的。

在群的定义中只包含一种运算。现在我们提出一种比群更复杂一点的代数结构，这就是所谓的环。它包含两种运算。

定义 9.3.16 设在非空的集合 R 中定义了两种代数运算，其中一种称为加法，记为 $a+b$，另一种称为乘法，记为 ab。使得

(1) R 中的元素对于加法构成群，其单位元记为 0；

(2) R 中的元素对于乘法满足结合律：$a(bc) = (ab)c$；

(3) R 中的元素满足乘法关于加法的分配率

$$a(b+c)=ab+ac$$
$$(b+c)a=ba+ca$$

则 R 称为一个环。

定义 9.3.17 设 R 是一个环，如果 R 中存在一个元素 e 使得对环中任意元素 a 都有

$$ea=ae=a$$

则称 e 是 R 的单位元。如果 R 有单位元，就称 R 是有单位元的环。

定义 9.3.18 在有单位元 e 的环中，如果对元素 a 存在元素 b 使得

$$ab=ba=e$$

则称元素 a 是可逆的。

定义 9.3.19 设 a 是环 R 中的非零元，如果有非零元 b 使得 $ab=0$，则称 a 是左零因子，如果有非零元 b 使得 $ba=0$，则称 a 是右零因子。既没有左零因子又没有右零因子的环称为整环。

定义 9.3.20 如果环 R 的乘法是交换的，即对所有的 $a\in G, b\in G$ 都有 $ab=ba$，则称 R 为交换环。

定义 9.3.21 设环 R 具有单位元，至少含有两个元素并且每个非零元都是可逆的，那么 R 就称为体或除环。交换的体或除环称为域。

环有以下简单性质：

定理 9.3.9

(1) 设 a 是可逆元，那么适合 $ab=ba=e$ 的元素 b 是唯一的，因此可定义此唯一的元素为 a 的逆元；

(2) 在整环中成立消去律；

(3) 体一定是整环，因而在体中成立消去律。

证明 (1) $ab_1=b_1a, ab_2=b_2a$，那么 $b_1=b_1e=b_1(ab_2)=(b_1a)b_2=eb_2=b_2$。这就证明了(1)。

(2) 设 $a\neq 0, ab=ac$，那么 $ab-ac=0, a(b-c)=0$。因为 $a\neq 0$ 且环中没有零因子，所以 $b-c=0, b=c$。同理可证如果 $a\neq 0, ba=ca$，那么 $b=c$。这就证明了(2)。

(3) 设 R 是体，$a\neq 0, ab=ac$，那么由 R 是体，$a\neq 0$ 知 a 可逆。因此 $b=a^{-1}(ab)=0$，这就说明 R 中没有零因子，因此在 R 中成立消去律。

例 9.3.6 所有的偶数组成一个环，因为两个偶数的和、差与积仍是一个偶数。更一般的，整数 m 的所有倍数组成一个环，通常记为 mZ，但是 mZ 不是域。

例 9.3.7 所有形式为 $a+b\sqrt{2}$ 的数(其中 a,b 都是整数) 构成一个环。

例 9.3.8 所有形式为 $a+b\sqrt{2}$ 的数(其中 a,b 都是有理数)构成一个域。通常记为 $R(\sqrt{2})$。$R(\sqrt{2})$ 对于加减法显然是封闭的。现在证明它对乘除法也是封闭的。事实上

$$(a+b\sqrt{2})(c+d\sqrt{2})=(ac+2bd)+(ad+bc)\sqrt{2}$$

由 a,b,c,d 都是有理数,显然可以得出 $ac+2bd,ad+bc$ 也是有理数。这就说明 $R(\sqrt{2})$ 对于乘法是封闭的。

又设 $a+b\sqrt{2}\in R(\sqrt{2})$,那么因为$\sqrt{2}$ 是无理数,而 a,b 都是有理数,因此 $a+b\sqrt{2}\neq 0,a-b\sqrt{2}\neq 0,a^2-2b^2\neq 0$,而

$$\frac{c+d\sqrt{2}}{a+b\sqrt{2}}=\frac{(a-b\sqrt{2})(c+d\sqrt{2})}{(a-b\sqrt{2})(a+b\sqrt{2})}=\frac{ac-2bd}{a^2-2b^2}+\frac{ad-bc}{a^2-2b^2}\sqrt{2}$$

由 a,b,c,d 都是有理数,显然可以得出$\frac{ac-2bd}{a^2-2b^2},\frac{ad-bc}{a^2-2b^2}$也是有理数。这就说明 $R(\sqrt{2})$ 对于除法是封闭的。

由各种类型的数组成的环和域称为数环和数域。所有的数环必包含零,因为一切数环的加群的单位元就是零。所有的数域都必包含有理数域。换句话说,有理数域是最小的数域。事实上,设 P 是一个数域。因为 P 中至少包含两个数,所以 P 中除了 0 之外,还一定包含一个不为 0 的数 a,因为 $a\neq 0$,所以 a 有逆,但是 a 是一个数,所以 a 的逆就是$\frac{1}{a}$,这就是说,对一切 $a\in P,a\neq 0$,必有 $\frac{1}{a}\in P$。因此 $a\cdot\frac{1}{a}=1\in P$。于是由加法的封闭性可以得出所有的整数都在 P 中,然后由 $a\cdot b^{-1}=\frac{a}{b}$ 又可以得出所有的有理数也都在 P 中。

为了给出一个不交换的环和有零因子的环的例子,我们下面引入矩阵的概念,至于矩阵的用途,在本书中就不讨论了。

定义 9.3.22 一个 n 元的有序的数组称为一个 n 维向量。以行的形式排列的 n 元有序数组称为行向量,记为$(a_1,a_2,\cdots,a_n)$,以行列的形式排列的 n 元有序数组称为列向量,记为

$$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}$$

定义 9.3.23 设 a 是一个 n 维行向量,b 是一个 n 维列向量,那么

$$a_1b_1+a_2b_2+\cdots+a_nb_n$$

称为 a,b 的内积,记为 $a\cdot b$。

定义 9.3.24 把 mn 个数排成如下的 m 行,n 列的表

$$A=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

称为一个 $m\times n$ 阶的矩阵。上面这个矩阵也可以用行向量和列向量写成

$$A=\begin{pmatrix} A_1 \\ A_2 \\ \vdots \\ A_m \end{pmatrix}$$

或

$$A=(B_1,B_2,\cdots,B_n)$$

其中

$$A_i=(a_{i1},a_{i2},\cdots,a_{in}),B=\begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{pmatrix}$$

定义 9.3.25 设 A 和 B 都 $m\times n$ 是阶的矩阵，且

$$A=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix},B=\begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & & \vdots \\ b_{m1} & b_{m2} & \cdots & b_{mn} \end{pmatrix}$$

那么 $m\times n$ 阶的矩阵

$$C=\begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} & \cdots & a_{1n}+b_{1n} \\ a_{21}+b_{21} & a_{22}+b_{22} & \cdots & a_{2n}+b_{2n} \\ \vdots & & & \vdots \\ a_{m1}+b_{m1} & a_{m2}+b_{m2} & \cdots & a_{mn}+b_{mn} \end{pmatrix}$$

称为 A 和 B 的和，记为 $C=A+B$。

定义 9.3.26 设矩阵 A 的行向量的维数与矩阵 B 的列向量的维数相等(都等于 s)。

$$A=\begin{pmatrix} A_1 \\ A_2 \\ \vdots \\ A_m \end{pmatrix}=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1s} \\ a_{21} & a_{22} & \cdots & a_{2s} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{ms} \end{pmatrix}$$

$$B=(B_1,B_2,\cdots,B_n)=\begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & & \vdots \\ b_{s1} & b_{s2} & \cdots & b_{sn} \end{pmatrix}$$

那么 $m \times n$ 阶的矩阵

$$C=\begin{pmatrix} A_1\cdot B_1 & A_1\cdot B_2 & \cdots & A_1\cdot B_n \\ A_2\cdot B_1 & A_2\cdot B_2 & \cdots & A_2\cdot B_n \\ \vdots & \vdots & & \vdots \\ A_m\cdot B_1 & A_m\cdot B_2 & \cdots & A_m\cdot B_n \end{pmatrix}$$

称为 A 与 B 的乘积，记为 $C=AB$。把 C 的第 i 行第 j 列处的元素 c_{ij} 明确写出来就是

$$c_{ij}=A_i\cdot B_j=a_{i1}b_{1j}+a_{i2}b_{2j}+\cdots+a_{in}b_{nj}$$

为了今后书写的方便，我们再定义一个概念：

定义 9.3.27 设 A 是一个矩阵，k 是一个实数。那么符号 kA 表示将 A 中所有元素都乘以 k 所得的矩阵。

定义 9.3.28 设 A 是一个 $m\times n$ 阶矩阵。

$$A=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

那么 $n\times m$ 阶矩阵

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{m1} \\ a_{21} & a_{22} & \cdots & a_{m2} \\ \vdots & \vdots & & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{mn} \end{pmatrix}$$

称为 A 的转置矩阵，记为 A' 或 A^{T}。

利用转置矩阵的符号，我们今后可把向量都写成行向量，但需要用到列向量时，只须把它写成行向量的转置即可。

下面我们给出几个矩阵的性质。

定理 9.3.10

(1) 设 k,h 表示数量，A,B 表示矩阵，那么数量和矩阵的乘法满足以下规律

$$(k+h)A=kA+hA$$
$$k(A+B)=kA+kB$$

$$k(hA) = (kh)A$$
$$1 \cdot A = A$$
$$k(AB) = (kA)B = A(kB)$$

(2) 设 k,h 表示数量，$E_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$，那么 E_n 满足以下等式

$$A_{mn}E_n = A_{mn}$$
$$E_nA_{mn} = A_{mn}$$
$$kA = (kE)A = A(kE)$$
$$kE + hE = (k+h)E$$
$$(kE)(hE) = (kh)E$$

其中 E,A,B 的阶数只须使得以上各式均有意义即可。

(3) 矩阵的加法和乘法满足以下规律。

加法结合律：$A + (B + C) = (A + B) + C$。

加法交换律：$A + B = B + A$。

存在加法单位元：$A + 0 = A = 0 + A$，其中 0 表示一个与 A 的阶数相同，而元素全为 0 的矩阵。

任一矩阵对加法运算存在逆元：设 $-A = (-1)\cdot A$，那么

$$A + (-A) = (-A) + A = 0$$

乘法对于加法的分配律：$A(B + C) = AB + AC$；$(B + C)A = BA + BC$。

乘法结合律：$(AB)C = A(BC)$。

证明　我们只证明乘法结合律，其余规律都很显然或容易证明。

设 $A = [a_{ij}]_{sm}$，$B = [b_{jk}]_{mn}$，$C = [c_{kh}]_{nr}$，$V = AB = [v_{ik}]_{sn}$，$W = BC = [w_{jh}]_{mr}$。其中

$$v_{ik} = a_{i1}b_{1k} + a_{i2}b_{2k} + \cdots + a_{im}b_{mk}, i = 1,2,\cdots,s, k = 1,2,\cdots,n$$
$$w_{jh} = b_{j1}c_{1h} + b_{j2}c_{2h} + \cdots + b_{jn}c_{nh}, j = 1,2,\cdots,m, h = 1,2,\cdots,r$$

由于 $(AB)C = VC$，而 VC 中第 i 行第 h 列处的元素为

$$\sum_{k=1}^{n} v_{ik}c_{kh} = \sum_{k=1}^{n}\left(\sum_{j=1}^{m} a_{ij}b_{jk}\right)c_{kh} = \sum_{k=1}^{n}\sum_{j=1}^{m} a_{ij}b_{jk}c_{kh}$$

另一方面由于 $A(BC) = AW$，而 AW 中第 i 行第 h 列处的元素为

$$\sum_{j=1}^{m} a_{ij}w_{jh} = \sum_{j=1}^{m} a_{ij}\left(\sum_{k=1}^{n} b_{jk}c_{kh}\right)c_{kh} = \sum_{j=1}^{m}\sum_{k=1}^{n} a_{ij}b_{jk}c_{kh}$$

由于上面的两个和都是有限项的和，所以可以交换求和的顺序，也就是

$$\sum_{k=1}^{n}\sum_{j=1}^{m} a_{ij}b_{jk}c_{kh} = \sum_{j=1}^{m}\sum_{k=1}^{n} a_{ij}b_{jk}c_{kh}$$

这说明$(AB)C$和$A(BC)$相应处的元素是完全相同的，因而$(AB)C = A(BC)$。这就证明了结合律。

例 9.3.9 全体$n \times n$矩阵的集合M_n构成一个有单位元的，不可交换的，含有(左右)零因子的环。

由定理9.3.10知矩阵对于加法构成一个群，满足乘法结合律和乘法对于加法的分配律，而且对于这两种运算都封闭，因此M_n是一个环。在此环中，E_n显然是乘法单位元。

设A是左下角为1，其余元素全为0的矩阵，B是右上角为1，其余元素全为0的矩阵。

$$A = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 1 & 0 & \cdots & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & 0 & \cdots & 1 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}$$

那么易证 $$AB = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}, BA = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}$$

因此M_n是不可交换的。

另外易证$A^2 = B^2 = \mathbf{0}$(这里的$\mathbf{0}$表示元素全为0的矩阵)，因此M_n中存在着(左右)零因子。

习题 9.3

1. 设$\mathbf{R}$是全体实数的集合，$M = \{(a,b) \mid a \in \mathbf{R}, b \in \mathbf{R}, a \neq 0\}$。在$M$上定义运算如下

$$(a,b) \cdot (c,d) = (ac, ad + b)$$

证明：M在上述运算下构成一个群。

2. (1) 写出正六边形的对称群；

(2) 写出正四面体的对称群。

3. 设

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}, B = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}$$

(1) 把A，B分解成轮换的乘积；

(2) 求AB，$A^{-1}BA$，A^2，A^3。

4. 证明：任何一个置换都能分解成一些对换的乘积，而分解式中对换的个数的奇偶性与分解式无关。因此可把全体置换分为两类：分解式中含有偶数个

对换的置换称为偶置换，分解式中含有奇数个对换的置换称为奇置换。

5. 证明：全体奇置换的集合 A_n 构成一个群，但是全体偶置换的集合不构成群。

6. 证明：$[A_n:1]=\frac{n!}{2}$。（A_n 的意义见 9.4，9.5）

7. 设 $\sigma=(1\,2\,3\,4)(5\,6\,7\,8)$，$\tau=(1\,6\,3\,8)(5\,2\,7\,4)$，证明：$\sigma\tau=\tau\sigma$ 并证明它们在 S_8 中生成一个 8 阶的子群。

8. 证明置换群中元素 aba^{-1} 可以这样得出：把 b 分解成不相交的轮换的乘积，然后把其中出现的号码全换成他们在 a 下的像。利用这一事实对

$$a=(2\,3\,4\,5),b=(1\,2)(3\,4\,5)$$

计算 aba^{-1}。

9. 证明：

(1) $S_n(n>1)$ 可由 $(1\,2)$，$(1\,3)$，$\cdots$，$(1\,n)$ 生成；

(2) $A_n(n>2)$ 可由 $(1\,2\,3)$，$(1\,2\,4)$，$\cdots$，$(1\,2\,n)$ 生成。

10. 设 G 是一非空集合，在 G 中可定义一种称为乘法的运算，具有以下性质：

(1) 满足乘法结合律；

(2) 对所有的 $a\in G,b\in G$，方程 $ax=b$ 和方程 $ya=b$ 都有解。

证明：G 是一个群。

11. 设 G 是一非空集合，在 G 中可定义一种称为乘法的运算，具有以下性质：

(1) 满足乘法结合律；

(2) 成立左消去律和右消去律。

证明：G 是一个群。

12. 证明：阶小于 6 的群必定是交换群。并举例说明存在 6 阶的非交换群。

13. 证明：如果群 G 中每个元素 x 都适合 $x^2=e$，则 G 是交换群。

14. 证明：群 G 的中心 $C(G)$ 也是一个群。

15. 设 a 是群 G 中的一个任意元素，$G(a)=\{b\mid ab=ba,b\in G\}$（即 $G(a)$ 是由 G 中所有与 a 可交换的元素组成的集合）。证明：$G(a)$ 也是一个群。

16. 写出 12 阶循环群的全部子群。

17. 证明：有理数加群不是有限生成的。

18. 设 G 为一交换群，$a\in G,b\in G$，a,b 的阶分别为 m,n。证明：ab 的阶为 mn。

19. 设 $G=(a)$ 是 n 阶循环群，证明：$G_1=(a^m)$ 的阶是 $\frac{n}{(m,n)}$。

20. 证明：阶为素数的群一定是循环群。

21. 如果群 G 中元素 a,b 满足关系 $b = c^{-1}ac$，其中 c 为 G 中某一元素，则称 b 共轭于 a。证明：共轭关系└是等价关系，即共轭满足以下 3 条性质：

(1) 反身性：$a \sim a$；

(2) 对称性：如果 $a \sim b$，那么 $b \sim a$；

(3) 传递性：如果 $a \sim b, b \sim c$，那么 $a \sim c$。

因此可用共轭关系将 G 中元素分成互相等价的类，群 G 中与元素 a 共轭的所有元素组成的集合称为由 a 决定的共轭类。

22. 设 G 是有限群，$a \in G$，则由 a 决定的共轭类（见 21 题）中所含有的元素的个数就等于 $G(a)$（见 15 题）在 G 中的指数，因而是 G 的阶的因子。

23. 证明：阶为素数方幂 $p^n(n > 0)$ 的群的中心除了单位元外，必还含有不是单位元的元素。

24. 证明：15 阶群必定是可交换的。

25. 证明：有理数加群与整数加群不同构。

26. 如果环中有一个元素 $e \neq 0$ 使得 $e^2 = e$，则称 e 是幂等元。证明：整环中的幂等元必为单位元。

27. 如果环中有一个元素 a 使得对于任意 $x \in \mathbf{R}$ 都有 $ax = x$，则称 a 是 $\mathbf{R}$ 的左单位元。证明：如果在 $\mathbf{R}$ 中左单位元是唯一的，那么左单位元就是单位元。

28. 证明：零因子不可能是可逆的。

29. 证明：任一含有非零元的有限整环是体。

30. 证明：有理数的自同构只能是恒同映射，实数域的自同构也只能是恒同映射。

31. 设 R 是有单位元的环，证明：如果 R 中元素 u 拥有不止一个右逆元，则它就有无数个右逆元。

32. 设环 R 中的任意元素 x 满足 $x^3 = x$，证明：R 一定是可交换的。

9.4 整数的推广：各种复整数

我们已经知道，整数有很多独特的性质，并且通过研究这些性质，可以得出很多有意思的结果。现在我们来考虑整数是否能够推广的问题。在历史上，推广整数的意义是和一些非常著名的问题例如费马问题联系在一起的。

最自然的推广是首先考虑所有形如 $a + bi$ 的数，其中 a,b 都是普通的整数。我们称这种数为复整数或高斯整数。复整数的全体记为 G。为避免混淆，以后我们将称普通的整数为有理整数。

普通的整数的一切讨论是从整除这个概念开始的。因此我们也首先来看看

在 G 中是否也能定义这一概念。显然 G 是一个整环，所以我们可以把整环看成是整数的推广。以下的许多定义对任意整环也有意义，因此在以下的讨论中，如果讨论的内容可以适合任意整环我们就用整环 M 来代替 G，这时所作的讨论当然也适用于 G，如果讨论的内容只适合 G，我们就在讨论中使用 G 这个符号。

定义 9.4.1 设 $\alpha \in M, \beta \in M$，如果存在 $\gamma \in M$，使得 $\beta = \alpha\gamma$，则称 α 整除 β，记为 $\alpha \mid \beta$。α 称为 β 的因数（也称约数或除数），β 称为 α 的倍数。如果不存在这样的 γ，则称 α 不能整除 β，记为 $\alpha \nmid \beta$。

在有理整数中，接下去的事情是，只讨论正整数，并且在正整数中，首先区分出 1，素数与合数三个范畴。所有这些事都和单位数有关。在有理整数中，单位数的概念比较简单，只有 1 和 -1。在 G 以及其他广义的整数中单位数就不这么简单了，由此将首先引出以下一些新的概念。

定义 9.4.2 如果 ϵ 和 ϵ^{-1} 都是 M 中的元素，则称 ϵ 是 M 中的单位数。

显然，单位数不等于 0，并且单位数的乘积和倒数仍是单位数。

下面出现了一个在普通整数中没有的概念。

定义 9.4.3 设 $\alpha \in M, \beta \in M, \varepsilon$ 是 M 中的单位数。如果 $\beta = \epsilon\alpha$，则称 α，β 是 M 中的相伴数（简称相伴数），或 β 与 α 相伴。

显然，相伴数是对称的，即如果 β 与 α 相伴，那么 α 也与 β 相伴。

原来有理整数中的素数概念现在分化成两个概念：

定义 9.4.4 设 $\alpha \in M$，α 不等于 0 也不是单位数，ϵ 是 M 中的单位数。如果 α 除了单位数和本身的相伴数之外没有其他因数，则称 α 是不可约数。

定义 9.4.5 设 $\pi \in M$，π 不等于 0 也不是单位数。如果对任意的 $\alpha \in M$，$\beta \in M$，从 $\pi \mid \alpha\beta$ 可以得出 $\pi \mid \alpha$ 或 $\pi \mid \beta$，则称 π 是一个素数。

原来有理整数中的互素这个概念，现在也分化为两个概念：

定义 9.4.6 设 $\alpha, \beta, \cdots, \gamma \in M$，如果 $\alpha, \beta, \cdots, \gamma$ 除了单位元外，没有其他公因数，就称 $\alpha, \beta, \cdots, \gamma$ 是既约的。

定义 9.4.7 设 $\alpha, \beta, \cdots, \gamma \in M$，如果存在 $x, y, \cdots, z \in M$ 使得

$$x\alpha + y\beta + \cdots + z\gamma = 1$$

则称 $\alpha, \beta, \cdots, \gamma$ 是互素的。

从整除的概念又可以导出公因数和公倍数的概念。

定义 9.4.8 设 $\alpha \in M, \beta \in M$，如果有 $\delta \in M$ 使得 $\delta \mid \alpha, \delta \mid \beta$，则称 δ 是 α, β 的公因（约）数。一般，如果 $\alpha, \beta, \cdots, \gamma \in M, \delta \in M$，而 $\delta \mid \alpha, \delta \mid \beta, \cdots$，$\delta \mid \gamma$，则称 δ 是 $\alpha, \beta, \cdots, \gamma$ 的公因（约）数。

定义 9.4.9 设 $\alpha, \beta, \cdots, \gamma \in M$，且均不为 0，如果存在 $\lambda \in M$，使得 $\alpha \mid \lambda$，$\beta \mid \lambda, \cdots, \gamma \mid \lambda$，则称 λ 是 $\alpha, \beta, \cdots, \gamma$ 的公倍数。

在有理整数中，有了以上这些概念后，下边就该定义我们很熟悉的“最大公

因数”和“最小公倍数”这两个概念了，这是两个非常重要的概念，在有理整数中，接下去的许多讨论都可借助这两个概念进行。

这里，我们遇到了推广整数工作时的第一个障碍。这是由于在有理整数中，存在着“大小”这一概念，而在 G 乃至一般的整环 M 中并没有这一概念。不过这一障碍还是可以克服的。克服的方法就是仿照集合论中最大、最小的概念，用包含来刻画大小。具体的办法是：

定义 9.4.10 设 $\alpha,\beta,\cdots,\gamma\in M$ 是不全为 0 的元素，如果存在 $\Delta\in M$ 满足

(1) Δ 本身是 $\alpha,\beta,\cdots,\gamma$ 的公因(约)数：$\Delta\mid\alpha,\Delta\mid\beta,\cdots,\Delta\mid\gamma$；

(2) $\alpha,\beta,\cdots,\gamma$ 的任意公因(约)数 δ 都是 Δ 的因数。

那么就称 Δ 是 $\alpha,\beta,\cdots,\gamma$ 的最大公因(约)数，记为 $(\alpha,\beta,\cdots,\gamma)$。

定义 9.4.11 设 $\alpha,\beta,\cdots,\gamma\in M$，且均不为 0，如果存在 $\Lambda\in M$ 使得

(1) Λ 本身是 $\alpha,\beta,\cdots,\gamma$ 的公倍数：$\alpha\mid\Lambda,\beta\mid\Lambda,\cdots,\gamma\mid\Lambda$；

(2) Λ 整除 $\alpha,\beta,\cdots,\gamma$ 的任何公倍数 λ。

那么就称 Λ 是 $\alpha,\beta,\cdots,\gamma$ 的最小公倍数，记为 $[\alpha,\beta,\cdots,\gamma]$。

由于在下面这个定理中，要列举的性质太多，所以我们改变以往叙述完定理之后再加以证明的方式，而采取随时加以说明或证明的方式。

定理 9.4.1 整环有以下性质：

(1) $\alpha\mid\beta\Leftrightarrow\varepsilon_1\alpha\mid\varepsilon_2\beta$，其中 $\varepsilon_1,\varepsilon_2$ 都是单位数。

(2) $\alpha\mid\beta,\beta\mid\gamma\Rightarrow\alpha\mid\gamma$。

(3) $\delta\mid\alpha,\delta\mid\beta,\cdots,\delta\mid\gamma$，对任意 $x,y,\cdots,z\in M,\delta\mid x\alpha+y\beta+\cdots+z\gamma$。

(4) 设 $\mu\neq0$，则 $\alpha\mid\beta\Leftrightarrow\mu\alpha\mid\mu\beta,\alpha=\beta\Leftrightarrow\mu\alpha=\mu\beta$。

(5) 设 $\alpha\neq0,\beta\neq0$，那么 $\alpha\mid\beta,\beta\mid\alpha\Leftrightarrow\beta=\varepsilon\alpha$，其中 ε 是单位数。

以上几条性质的证明都十分简单容易，故略去。

下面一些性质涉及最大公因数与最小公倍数的概念，在普通整数中，因为只有两个单位数，我们可以把讨论只限于正整数范围内，这时单位数，最大公因数与最小公倍数都是唯一的。而在一般整环中，并无法一般地把整环作类似于普通整数那样的划分的方法，因此单位数、最大公因数与最小公倍数都不是唯一的，而是一个集合，因此下面的单位数，最大公因数与最小公倍数的符号都表示一个集合。而性质中所说的不变，也是表示这些集合不变。

另外，在普通整数中最大公因数与最小公倍数都是一定存在的，而且可以证明对于普通整数来说最大公因数与最小公倍数的老的定义与新的定义是一致的。而在一般的整环中，有可能发生一些元素的最大公因数或最小公倍数在新的定义下不存在的情况，因此下面含有最大公因数与最小公倍数的等式时只在式中这些概念都存在时才有意义，否则就没有意义。

(6) 把 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 中的任意数换成其相伴数，它们的最大公因数不变；$\alpha_1,\alpha_2,\cdots,\alpha_n$ 的最大公因数与 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 的排列次序及分组形式（只要在所作的分组下，最大公因数存在）无关。

在 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 中任何一个数上加上 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 的任意线性组合后，最大公因数不变，即对任意 $x_1,x_2,\cdots,x_n\in M$ 有

$$(\alpha_1,\alpha_2,\cdots,\alpha_i,\cdots,\alpha_n)=(\alpha_1,\alpha_2,\cdots,\alpha_i+x_1\alpha_1+x_2\alpha_2+\cdots+x_n\alpha_n,\cdots\alpha_n)$$

我们只证明 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 的最大公因数与分组形式无关。

设 $(\alpha_1,\alpha_2,\cdots,\alpha_r)$，$(\alpha_{r+1},\alpha_{r+2},\cdots,\alpha_n)$ 存在，于是可设 $(\alpha_1,\alpha_2,\cdots,\alpha_r)=\Delta_1$，$(\alpha_{r+1},\alpha_{r+2},\cdots,\alpha_n)=\Delta_2$。如果 (Δ_1,Δ_2) 存在，则可设 $(\Delta_1,\Delta_2)=\Delta$。那么由 $\Delta\mid\Delta_1$，$\Delta\mid\Delta_2$ 得出 $\Delta\mid\alpha_1,\Delta\mid\alpha_2,\cdots,\Delta\mid\alpha_n$，另一方面，对任意 $\delta\mid\alpha_1,\delta\mid\alpha_2,\cdots,\delta\mid\alpha_n$ 必有 $\delta\mid\Delta_1,\delta\mid\Delta_2$，因而有 $\delta\mid\Delta$，这就说明 $(\alpha_1,\alpha_2,\cdots,\alpha_n)$ 存在，且 $(\alpha_1,\alpha_2,\cdots,\alpha_n)=\Delta$，即

$$((\alpha_1,\alpha_2,\cdots,\alpha_r),(\alpha_{r+1},\alpha_{r+2},\cdots,\alpha_n))=(\alpha_1,\alpha_2,\cdots,\alpha_n)$$

不过要注意，可能在某种分组下，这种分组的最大公因数不存在，那么此时，上式就无意义。

(7) $\alpha,\beta,\cdots,\gamma$ 既约的充分必要条件是 $(\alpha,\beta,\cdots,\gamma)=\epsilon$，其中 ϵ 是单位数。

这一性质的证明也十分简单，故略去。

(8) 设 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 不全为0，$(\alpha_1,\alpha_2,\cdots,\alpha_n)$ 存在，δ 是 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 的任一公因数，μ 是 M 中任意元素，那么

$$\left(\frac{\alpha_1}{\delta},\frac{\alpha_2}{\delta},\cdots,\frac{\alpha_n}{\delta}\right)=\frac{(\alpha_1,\alpha_2,\cdots,\alpha_n)}{\delta}$$

$$\mu(\alpha_1,\alpha_2,\cdots,\alpha_n)=(\mu\alpha_1,\mu\alpha_2,\cdots,\mu\alpha_n)$$

特别

$$\left(\frac{\alpha_1}{(\alpha_1,\alpha_2,\cdots,\alpha_n)},\frac{\alpha_2}{(\alpha_1,\alpha_2,\cdots,\alpha_n)},\cdots,\frac{\alpha_n}{(\alpha_1,\alpha_2,\cdots,\alpha_n)}\right)=\epsilon$$

我们以 $n=2$ 时的情况为例加以证明，一般情况可以类似证明。

设 $(\alpha_1,\alpha_2)=\Delta$，那么由最大公因数的定义可知，$\delta\mid\Delta$。于是可设 $\Delta_1=\frac{\Delta}{\delta}$。由 $\Delta\mid\alpha_1,\Delta\mid\alpha_2$ 得出 $\Delta_1=\frac{\Delta}{\delta}\Big|\frac{\alpha_1}{\delta}$，$\Delta_1=\frac{\Delta}{\delta}\Big|\frac{\alpha_2}{\delta}$。另一方面对 $\frac{\alpha_1}{\delta},\frac{\alpha_2}{\delta}$ 的任意公因数 δ_1，由 $\delta_1\mid\frac{\alpha_1}{\delta}$，$\delta_1\mid\frac{\alpha_2}{\delta}$ 得出 $\delta_1\delta\mid\alpha_1$，$\delta_1\delta\mid\alpha_2$，再由 Δ 是 α_1,α_2 的最大公因数的定义可知 $\delta_1\delta\mid\Delta$，因而有 $\delta_1\mid\Delta_1$。因此由最大公因数的定义就得出

$$\left(\frac{\alpha_1}{\delta},\frac{\alpha_2}{\delta}\right)=\Delta_1=\frac{\Delta}{\delta}=\frac{(\alpha_1,\alpha_2)}{\delta}$$

如果 $\mu=0$，$\mu(\beta_1,\beta_2,\cdots,\beta_n)=(\mu\beta_1,\mu\beta_2,\cdots,\mu\beta_n)$ 显然成立。因此以下可设 $\mu\neq0$，在

$$\left(\frac{\beta_1}{\mu},\frac{\beta_2}{\mu},\cdots,\frac{\beta_n}{\mu}\right)=\frac{(\beta_1,\beta_2,\cdots,\beta a_n)}{\mu}$$

中令 $\beta_i=\mu\alpha_i$ 就得出

$$\mu\mid(\beta_1,\beta_2,\cdots,\beta_n)$$

以及
$$(\alpha_1,\alpha_2,\cdots,\alpha_n)=\frac{(\mu\alpha_1,\mu\alpha_2,\cdots,\mu\alpha_n)}{\mu}$$

因而
$$\mu(\alpha_1,\alpha_2,\cdots,\alpha_n)=(\mu\alpha_1,\mu\alpha_2,\cdots,\mu\alpha_n)$$

注意这一性质虽然与普通整数的相应性质在形式上很类似，但是有一点实质性的不同之处在于，对于普通的整数，无论$\left(\frac{\alpha_1}{\delta},\frac{\alpha_2}{\delta},\cdots,\frac{\alpha_n}{\delta}\right)$还是$(\alpha_1,\alpha_2,\cdots,\alpha_n)$都一定存在。而在一般的整环中，有可能发生一些元素的最大公因数不存在的情况。因此必须首先假定$(\alpha_1,\alpha_2,\cdots,\alpha_n)$的存在性。

(9) 把 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 中的任意数换成其相伴数，它们的最小公倍数不变；$\alpha_1,\alpha_2,\cdots,\alpha_n$ 的最小公倍数与 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 的排列次序及分组形式（只要在所作的分组下，最小公倍数存在）无关。

证明与性质(6)类似。

(10) 设 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 都不为 0，$\mu\neq0$ 是一个实数，则

$$[\mu\alpha_1,\mu\alpha_2,\cdots,\mu\alpha_n]=\mu[\alpha_1,\alpha_2,\cdots,\alpha_n]$$

我们只证 $n=2$ 时的情况，一般情况可以类似证明。

设$[\mu a_1,\mu a_2]$存在，于是可设$[\mu a_1,\mu a_2]=\Lambda$。根据最小公倍数的定义可知 $\mu a_1\mid\Lambda$，因此 $\mu\mid\Lambda$。于是可设 $\Lambda_1=\frac{\Lambda}{\mu}$。由 $\mu a_1\mid\Lambda,\mu a_2\mid\Lambda$ 得出 $a_1\mid\Lambda_1,a_2\mid\Lambda_1$，另一方面，对任意 a_1,a_2 的公倍数 λ，由 $a_1\mid\lambda,a_2\mid\lambda$ 可以得出 $\mu a_1\mid\mu\lambda$，$\mu a_2\mid\mu\lambda$，因而由 Λ 是 $\mu a_1,\mu a_2$ 的最小公倍数的定义有 $\Lambda\mid\mu\lambda$，因而

$$\Lambda_1=\frac{\Lambda}{\mu}\left|\frac{\mu\lambda}{\mu}\right.=\lambda$$

再由最小公倍数的定义就得出

$$[a_1,a_2]=\lambda=\frac{\Lambda}{\mu}=\frac{[\mu a_1,\mu a_2]}{\mu}$$

因此
$$\mu[a_1,a_2]=[\mu a_1,\mu a_2]$$

(11) 设 $\alpha,\beta\in M$，如果$[\alpha,\beta]$存在，则(α,β)也存在，且$(\alpha,\beta)=\frac{\alpha\beta}{[\alpha,\beta]}$。

由$[\alpha,\beta]$存在可设 $\Delta=\frac{\alpha\beta}{[\alpha,\beta]}$。由 $\beta\mid[\alpha,\beta]$，$\alpha\mid[\alpha,\beta]$ 可以得出 $\alpha\beta\mid\alpha[\alpha,\beta]$，$\alpha\beta\mid\beta[\alpha,\beta]$，由此得出

$$\Delta=\frac{\alpha\beta}{[\alpha,\beta]}\left|\alpha,\Delta=\frac{\alpha\beta}{[\alpha,\beta]}\right|\beta$$

另一方面,对于 α,β 的任意公因数 δ 又有

$$\delta\left(\frac{\alpha}{\delta}\right)\left(\frac{\beta}{\delta}\right)=\frac{\alpha\beta}{\delta}=\frac{\Delta[\alpha,\beta]}{\delta}=\Delta\left[\frac{\alpha}{\delta},\frac{\beta}{\delta}\right]$$

因此

$$\frac{\Delta}{\delta}=\frac{\left(\frac{\alpha}{\delta}\right)\left(\frac{\beta}{\delta}\right)}{\left[\frac{\alpha}{\delta},\frac{\beta}{\delta}\right]}$$

由最小公倍数的定义即得 $\delta\mid\Delta$。因此再由最大公约数的定义就得出

$$\frac{\alpha\beta}{[\alpha,\beta]}=\Delta=(\alpha,\beta)$$

(12) 如果 $\alpha,\beta,\cdots,\gamma$ 互素,则 $\alpha,\beta,\cdots,\gamma$ 既约。

(13) 素数一定是不可约数。

(14) 如果 α,β 互素,$\alpha\mid\beta\gamma$,则 $\alpha\mid\gamma$。

(15) 设 α,β 互素,则 α,γ 互素(或既约)的充分必要条件是 $\alpha,\beta\gamma$ 互素(或既约)。

(16) 如果 α,β 互素,则$[\alpha,\beta]=\varepsilon\alpha\beta$。

(17) 设 π 是素数,π,α 既约,π,β 既约,则 $\pi,\alpha\beta$ 既约。

(18) 设 α 可表为素数的乘积,则这个表示式在不计次序和相伴的意义下是唯一的。

以上 7 条性质或者从定义本身容易推出,或者可以仿照第三章中相应命题的证明来证明,因此省略。

上面这 18 条性质是对一般的整环都成立的,下面的一些性质则不是这样。因此,我们从现在开始,需要研究一些 G 中特有的性质,在这些性质中,最重要的是下面两条定理。为此,我们需先给出以下定义:

定义 9.4.12 设 $\alpha=x+y\mathrm{i}$ 是 G 中任意元素,则称 $\alpha\bar{\alpha}=x^2+y^2$ 为 α 在 G 中的模或范数,记为 $N(\alpha)$。

注意,α 在 G 中的模与 α 作为一个复数的模稍有不同。作为复数,α 的模是 $|\alpha|=\sqrt{x^2+y^2}$,而作为 G 中的元素,α 的模 $N(\alpha)$ 总是一个整数。易证模有下面的性质:

引理 9.4.1 在 G 中,模有如下性质:

(1) α 的模 $N(\alpha)$ 总是一个整数;

(2) $N(\alpha)=\alpha\bar{\alpha}$;

(3) $N(\alpha\beta)=N(\alpha)N(\beta)$;

(4) $N(\alpha)=0$ 的充分必要条件是 $\alpha=0$;

(5) $N(\alpha)=1$ 的充分必要条件是是 α 单位数;

(6) α,β 是相伴数的充分必要条件是 $N(\alpha)=N(\beta)$。

定义 9.4.13 设 M 是整环,如果 M 中任意既不是 0 也不是单位数的元素 α 一定可以分解成有限个不可约元的乘积,则称 M 是可分解整环。

定理 9.4.2 G 是可分解整环。

证明 如果 α 本身就是不可约元,那么定理已经成立。如果 α 不是不可约元,那么必有 $\alpha_1\in G,\alpha_1\neq 0$ 使得 $\alpha_1\mid\alpha$,因此 $N(\alpha_1)\mid N(\alpha)$。由此得出 $1<N(\alpha_1)<N(\alpha)$,如果 α_1 本身就是不可约元,那么定理又已经成立。如果 α_1 不是不可约元,那么必有 $\alpha_2\in G,\alpha_2\neq 0$ 使得 $\alpha_2\mid\alpha_1$,因此 $N(\alpha_2)\mid N(\alpha_1)$。由此得出 $1<N(\alpha_2)<N(\alpha_1)<N(\alpha),\cdots$,如此进行下去,由于 $N(\alpha)$ 是有限的自然数,而上述步骤每进行一次,模至少要减小 1,因此应用上述步骤有限次后,必存在一个自然数 n,使得 $\alpha_n\mid\alpha_{n-1}$,而 α_n 已是不可约元。令 $\beta_1=\alpha_n$,则 β_1 已是不可约元。且 $N\left(\frac{\alpha}{\beta_1}\right)<N(\alpha)$,对 $N\left(\frac{\alpha}{\beta_1}\right)$ 继续应用上述步骤,又可经有限步分出 α 的第二个不可约因子 β_2,如此经过有限步后,就把 α 分解成了有限个不可约因子的乘积。

定理 9.4.3 G 中成立第二带余数除法,即对任意 $\alpha,\beta\in G,\alpha\neq 0$,一定存在 $\eta,\gamma\in G$,使得

$$\beta=\eta\alpha+\gamma,0\leqslant N(\gamma)<N(\alpha)$$

证明 设 $\frac{\beta}{\alpha}=r+s\mathrm{i}$,其中 r,s 都是有理数。设 u,v 分别是距离 r,s 最近的有理整数。那么显然就有

$$|u-r|\leqslant\frac{1}{2},|v-s|\leqslant\frac{1}{2}$$

现在令 $\eta=u+v\mathrm{i},\gamma=\beta-\alpha\eta$,因此 $\beta=\eta\alpha+\gamma$,则

$$\begin{aligned}N(\gamma)=N(\beta-\alpha\eta)=N(\alpha)N\left(\frac{\beta}{\alpha}-\eta\right)=\\ N(\alpha)N(r+s\mathrm{i}-u-v\mathrm{i})=\\ N(\alpha)N((r-u)+(s-v)\mathrm{i}=\\ ((r-u)^2+(s-v)^2)N(\alpha)\leqslant\\ \left(\left(\frac{1}{2}\right)^2+\left(\frac{1}{2}\right)^2\right)N(\alpha)\leqslant\frac{1}{2}N(\alpha)<N(\alpha)\end{aligned}$$

这就证明了定理。

由定理 9.4.3 可证下面的

定理 9.4.4(欧几里得算法) 任给 $\beta_0,\beta_1\in G,\beta_1\neq 0$ 一定可得如下的一组等式:

$$\beta_0=\eta_1\beta_1+\beta_2,0<N(\beta_2)<N(\beta_1),\eta_1,\beta_2\in G$$

$$\beta_1 = \eta_2\beta_2 + \beta_3, 0 < N(\beta_3) < N(\beta_2), \eta_2, \beta_3 \in G$$
$$\vdots$$
$$\beta_{n-1} = \eta_n\beta_n + \beta_{n+1}, 0 < N(\beta_{n+1}) < N(\beta_n), \eta_n, \beta_{n+1} \in G$$
$$\beta_n = \eta_{n+1}\beta_{n+1}, \qquad \eta_{n+1} \in G$$

证明　由定理 9.4.3 知，我们可依次进行定理中所示的除法，且有

$$N(\beta_1) > N(\beta_2) > \cdots \geqslant 1$$

（注意，如果在某一步中有 $\beta_i = 0$，则上述算法自动停止，因此，只要上述算法不停止，算式中的除数就始终不为 0，因而下一步的算式就是有意义的），所以，$\beta_1, \beta_2, \cdots$ 的范数是严格递减的。但是这些范数都是正整数，因此，或者在某一步有 $N(\beta_{i+1}) > 1, \beta_{i+1} \mid \beta_i$，因而算法到此结束，$n = i$；或者一直到最后出现 $N(\beta_{i+1}) = 1$，因而 β_{i+1} 是 G 中的单位数，这时显然也有 $\beta_{i+1} \mid \beta_i$，因而算法还是结束。总之，上述算法将在有限步内结束。这就证明了定理。

由此引出以下定义：

定义 9.4.14　如果在整环 M 中可定义一种范数 N，使得对此范数成立欧几里得算法，即对任意 $\beta_0, \beta_1 \in M, \beta_1 \neq 0$，一定可得如下的一组等式

$$\beta_0 = \eta_1\beta_1 + \beta_2, 0 < N(\beta_2) < N(\beta_1), \eta_1, \beta_2 \in M$$
$$\beta_1 = \eta_2\beta_2 + \beta_3, 0 < N(\beta_3) < N(\beta_2), \eta_2, \beta_3 \in M$$
$$\vdots$$
$$\beta_{n-1} = \eta_n\beta_n + \beta_{n+1}, 0 < N(\beta_{n+1}) < N(\beta_n), n_n, \beta_{n+1} \in M$$
$$\beta_n = \eta_{n+1}\beta_{n+1}, \qquad \eta_{n+1} \in M$$

则称 M 是欧几里得环。

由此得出

定理 9.4.5　G 是欧几里得环。

下面这个定理中所涉及的性质较多，因此我们仍采取定理 9.4.1 中的方法，对这些性质随时加以证明或说明。

定理 9.4.6　如果整环 M 是欧几里得环，则以下性质成立：

(1) 任给不全为 0 的 $\alpha_1, \alpha_2, \cdots, \alpha_n \in M$，$(\alpha_1, \alpha_2, \cdots, \alpha_n)$ 存在。

首先对 $n = 2$ 的情况证明这一性质成立。

不妨设 $\alpha_2 \neq 0$，在定理 9.4.4 中令 $\alpha_1 = \beta_0, \alpha_2 = \beta_1$，那么从算法中的等式中可以得出

$$\beta_{n+1} \mid \beta_n \mid \beta_{n-1} \mid \cdots \mid \beta_1 = \alpha_2 \mid \beta_0 = \alpha_1$$

因此 β_{n+1} 是 α_1, α_2 的公因数。另一方面，设 δ 是 α_1, α_2 的任意公因数，那么从 $\delta \mid \alpha_1 = \beta_0, \delta \mid \alpha_2 = \beta_1$ 和算法中的等式又可得出

$$\delta \mid \beta_1 \mid \beta_2 \mid \cdots \mid \beta_n \mid \beta_{n+1}$$

因而由最大公因数的定义就得出

$$(\alpha_1,\alpha_2)=\beta_{n+1}$$

对于一般的情况，不妨设 $\alpha_1\neq 0$，于是由对 $n=2$ 已证的结论知 (α_1,α_2) 存在，且 $(\alpha_1,\alpha_2)\neq 0$，因而 $\Delta=((\alpha_1,\alpha_2),\alpha_3)$ 存在，且 $\Delta\neq 0$。Δ 显然是 $\alpha_1,\alpha_2,\alpha_3$ 的公因数。现设 δ 是 $\alpha_1,\alpha_2,\alpha_3$ 的任意公因数，那么根据最大公因数的定义就得出 δ 是 (α_1,α_2) 的因数，因而是 Δ 的因数，再根据最大公因数的定义就得出 $\Delta=(\alpha_1,\alpha_2,\alpha_3)$，任后由数学归纳法就可得出(4)。

(2) 对任意不全为 0 的 $\alpha_1,\alpha_2,\cdots,\alpha_n\in M$，存在 $\lambda_1,\lambda_2,\cdots,\lambda_n\in M$，使得

$$(\alpha_1,\alpha_2,\cdots,\alpha_n)=\lambda_1\alpha_1+\lambda_2\alpha_2+\cdots+\lambda_n\alpha_n$$

在定理 9.4.4 中倒退回去，就可把 β_{n+1} 表为 β_0 和 β_1 的也就是 α_1 和 α_2 的线性组合，因而由性质(1) 就得出(2) 对于 $n=2$ 的情况成立。

因而根据(1) 中的证明和已证的结论知存在 $\mu_1,\mu_2\in M$ 及 $v_1,v_2\in M$ 使得

$$\begin{aligned}(\alpha_1,\alpha_2,\alpha_3)=((\alpha_1,\alpha_2),\alpha_3)&=\mu_1(\alpha_1,\alpha_2)+\mu_2\alpha_3=\\&\mu_1(v_1\alpha_1+v_2\alpha_2)+\mu_2\alpha_3=\\&\mu_1v_1\alpha_1+\mu_1v_2\alpha_2+\mu_2\alpha_3=\\&\lambda_1\alpha_1+\lambda_2\alpha_2+\lambda_3\alpha_3\end{aligned}$$

然后在由数学归纳法即可证明(2) 成立。

由(2) 和定义立刻得出：

(3) 如果 $\alpha_1,\alpha_2,\cdots,\alpha_n\in M$ 既约，则 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 互素。

(4) 设 ϵ 是环 M 中的单位数，$(\delta,\alpha)=\epsilon$，则 $(\delta,\alpha\beta)=(\delta,\beta)$。

当 $\delta=0$ 时，$\alpha=\epsilon$，结论显然成立。当 $\delta\neq 0$ 时，利用定理 9.4.1(8) 可以得出

$$\begin{aligned}(\delta,\beta)=(\delta,(\delta,\alpha)\beta)&=(\delta,(\delta\beta,\alpha\beta))=\\&(\delta,\delta\beta,\alpha\beta)=((\delta,\delta\beta),\alpha\beta)=\\&(\delta(1,\beta),\alpha\beta)=(\delta,\alpha\beta)\end{aligned}$$

特别，如果 $(\delta,\alpha)=\epsilon$，$(\delta,\beta)=\epsilon$，则 $(\delta,\alpha\beta)=\epsilon$。

(5) 设 ϵ 是环 M 中的单位数，$(\delta,\alpha)=\epsilon$，$\delta\mid\alpha\beta$，则 $\delta\mid\beta$。

从(4)，最大公因数的定义和 $\delta\mid\alpha\beta$ 得出 $\delta=(\delta,\alpha\beta)=(\delta,\beta)$，再由最大公因数的定义就得出 $\delta\mid\beta$。

(6) 设 π 是 M 中不可约元，$\pi\mid\alpha_1,\alpha_2,\cdots,\alpha_n$，则存在一个 α_i，$1\leqslant i\leqslant n$ 使得 $\pi\mid\alpha_i$。

只证 $n=2$ 的情况，一般情况类似可证。

设 π 是 M 中的不可约元，且 $\pi\mid\alpha\beta$，我们要证明必有 $\pi\mid\alpha$ 或 $\pi\mid\beta$。

由于 π 是 M 中不可约元，因此必有 $(\pi,\alpha)=\epsilon$ 或 π(因为根据不可约元的定义，π 的因数只有 ϵ 和 π)，而 $(\pi,\alpha)=\pi$ 的充分必要条件是 $\pi\mid\alpha$。因此如果 π 既

不能整除 α 又不能整除β，就必有$(\pi,\alpha)=\epsilon$，$(\pi,\beta)=\epsilon$，因而由(4)得出$(\pi,\alpha\beta)=\epsilon$。但是已知 $\pi\mid\alpha\beta$，因此$(\pi,\alpha\beta)=\pi$。这与$(\pi,\alpha\beta)=\epsilon$ 矛盾。因此必有 $\pi\mid\alpha$ 或 $\pi\mid\beta$。根据素数的定义，这就证明了 π 一定是素数。

由(6) 立刻得出

(7) M 中的不可约元一定是素数。

(8) 设 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 是 M 中全不为 0 的数，则$[\alpha_1,\alpha_2,\cdots,\alpha_n]$ 存在。

首先对 $n=2$ 的情况证明这一性质成立。

由(1) 可知(α_1,α_2) 存在。先设$(\alpha_1,\alpha_2)=1$。令 $\Lambda=\alpha_1\alpha_2$，那么显然有 $\alpha_1\mid\Lambda$，$\alpha_2\mid\Lambda$。现在设 λ 是α_1,α_2 的任意一个公倍数，则 $\alpha_1\mid\lambda$，因此 $\lambda=\alpha_1\gamma$。再由 λ 是α_1,α_2 的公倍数得出 $\alpha_2\mid\alpha_1\gamma$，因而由$(\alpha_1,\alpha_2)=1$，$\alpha_2\mid\alpha_1\gamma$ 和(5) 得出 $\alpha_2\mid\gamma$，因而 $\Lambda=\alpha_1\alpha_2\mid\alpha_1\gamma=\lambda$。因此根据最小公倍数的定义就得出$[\alpha_1,\alpha_2]=\Lambda=\alpha_1\alpha_2$，因而$[\alpha_1,\alpha_2]$ 存在。

对一般情况，由$\left(\frac{\alpha_1}{(\alpha_1,\alpha_2)},\frac{\alpha_2}{(\alpha_1,\alpha_2)}\right)=1$ 和上面已证明的结论就得出

$$\left(\frac{\alpha_1}{(\alpha_1,\alpha_2)},\frac{\alpha_2}{(\alpha_1,\alpha_2)}\right)=\frac{\alpha_1\alpha_2}{(\alpha_1,\alpha_2)^2}$$

因此$\left(\frac{\alpha_1}{(\alpha_1,\alpha_2)},\frac{\alpha_2}{(\alpha_1,\alpha2)}\right)$存在，再由定理 9.4.1(10)，(11) 就得出

$$[\alpha_1,\alpha_2]=(\alpha_1,\alpha_2)\left(\frac{\alpha_1}{(\alpha_1,\alpha_2)},\frac{\alpha_2}{(\alpha_1,\alpha_2)}\right)=\frac{\alpha_1\alpha_2}{(\alpha_1,\alpha_2)}$$

因而$[\alpha_1,\alpha_2]$ 存在。

对 $n=3$ 的情况。由对 $n=2$ 已证的结论知 $\Lambda=[[\alpha_1,\alpha_2],\alpha_3]$ 又意义。显然 Λ 是$\alpha_1,\alpha_2,\alpha_3$ 的公倍数。现在设 λ 是$\alpha_1,\alpha_2,\alpha_3$ 的任意公倍数，则由最小公倍数的定义知$[\alpha_1,\alpha_2]\mid\lambda$，$\alpha_3\mid\lambda$，因此 λ 也是$[\alpha_1,\alpha_2]$ 和 α_3 的公倍数。再次由最小公倍数的定义知 $\Lambda\mid\lambda$，于是仍由最小公倍数的定义就得出 $\Lambda=[\alpha_1,\alpha_2,\alpha_3]$，因而$[\alpha_1,\alpha_2,\alpha_3]$ 存在。以后用数学归纳法即可证明$[\alpha_1,\alpha_2,\cdots,\alpha_n]$ 存在。

定理 9.4.7(唯一分解式定理)　设环 M 是可分解整环同时又是欧几里得环，则 M 中任意既不是 0 也不是单位数的元素 α 一定可以分解成有限个不可约元的乘积

$$\alpha=\xi_1\xi_2,\cdots,\xi_r$$

且此分解式在不计次序和相伴时是唯一的。这就是说在不计次序时 α 一定可以唯一地表为

$$\alpha=\epsilon\eta_1^{r_1}\eta_2^{r_2}\cdots\eta_s^{r_s}$$

其中 $\eta_1,\eta_2,\cdots,\eta_s$ 是两两互不相伴的不可约元，ϵ 是单位数。

证明　由于 M 是可分解整环，因此分解式 $\alpha=\xi_1\xi_2\cdots\xi_r$ 存在。设 α 还有分

解式 $\alpha = \eta_1\eta_2\cdots\eta_s$。不妨设 $r \geqslant s$。由定理9.4.6(7)知 $\xi_1\xi_2,\cdots,\xi_r,\eta_1,\eta_2,\cdots,\eta_s$ 都是素数,由素数的定义知,从 $\eta_1 \mid \alpha = \xi_1\xi_2,\cdots,\xi_r$ 可以得出必有一个 ξ_i 使得 $\eta_1 \mid \xi_i$。不妨设 $i = 1$。由此及不可约元的定义就有 $\eta_1 = \epsilon_1\xi_1$,其中 ϵ_1 是单位数,因而 $\eta_2\cdots\eta_s = \epsilon_1\xi_2\cdots\xi_r$。同理又可得出 $\eta_2 = \epsilon_2\xi_2,\cdots$,依次类推,最后即得出 $r = s,\eta_i = \epsilon_i\xi_i, i = 1,2,\cdots,s$,这就证明了定理。

上面,我们已经一般地讨论了对一般的整环都成立的性质和只在 G 中成立的性质。但是为了能够具体地应用这些性质,我们还必须具体地确定 G 中的单位数是什么?不可约元或素数(上面已证,在 G 中,这两个概念是一致的)又是什么?第一个问题比较简单。

引理9.4.1 G 中只有4个单位数: $\pm 1, \pm \mathrm{i}$。

证明 设 $\epsilon = a + b\mathrm{i}$ 是 G 中的单位数,那么 $\epsilon = a + b\mathrm{i}$ 是 G 中的整数,因此 a,b 都是有理整数。由 ϵ^{-1} 也是 G 中整数和 $\epsilon\cdot\epsilon^{-1} = 1$ 得出 $N(\epsilon)N(\epsilon^{-1}) = N(\epsilon\epsilon^{-1}) = N(1) = 1$,由此得出

$$a^2 + b^2 = 1$$

从上面的式子容易得出只能有 $a^2 = 1, b = 0$ 或 $a = 0, b^2 = 1$,由此即可得出引理。

为了说明 G 中的素数是什么,我们需要下面的引理:

引理9.4.2 设 p 是形如 $4m + 1$ 的有理素数,则存在自然数 n,使 $p \mid n^2 + 1$。

证明 由条件得出 $p \equiv 1 \pmod 4$,因此

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1$$

因此同余式方程

$$x^2 \equiv -1 \pmod p$$

有解,这就证明了引理。

不过这种方法,只能证明存在自然数 n,使 $p \mid n^2 + 1$,而不能得出 n 的奇偶性,用下面的方法可进一步证明 n 一定是偶数,还不止如此,可以证明 n 一定可以表示成 $(2m)!$ 的形式。

考虑下面两个集合: $-1,-2,\cdots,-2m$ 和 $4m,4m-1,\cdots,2m+1$,由于上下两个集合中对应的元素之差都是 p,因此

$$4m(4m-1)\cdots(2m+1) \equiv (-1)(-2)\cdots(-2m) \equiv (2m)! \pmod p$$

在上式两边各乘以 $(2m)!$ 得

$$(4m)! \equiv ((2m)!)^2 \pmod p$$

令 $n = (2m)!$,那么由维尔逊定理就得出(见第三章定理3.9.13)

$$n^2 \equiv ((2m)!)^2 \equiv (4m)! \equiv (p-1)! \equiv -1 \pmod p$$

由此就得出 $p \mid n^2+1$。

引理 9.4.3 设 M 是欧几里得环，$\alpha \in M$，则如果 $N(\alpha)$ 是有理素数，那么 α 必是 M 中的素数。

证明 首先由 $N(\alpha)$ 是有理素数可知 $\alpha \neq 0$（否则 $N(\alpha)=0$ 不是有理素数，与假设矛盾）。我们证 α 必是 M 中的不可约元。假设不然，则 $\alpha = \beta\gamma$，其中 β，γ 都不是单位数，因此 $N(\beta)>1$，$N(\gamma)>1$，这就得出 $N(\alpha)=N(\beta)N(\gamma)$ 不是有理素数，与假设矛盾，因此 α 必是 M 中的不可约元。由于 M 是欧几里得环，因此由定理 9.4.6(7) 就得出 α 是 M 中的素数。

引理 9.4.4 任给 $\alpha \in G$，则 $\alpha \mid N(\alpha)$。

证明 由于在 G 中，$N(\alpha)=\alpha\bar{\alpha}$，故显然有 $\alpha \mid N(\alpha)$。

引理 9.4.5 设在 G 中 $N(\pi)=p$ 是一个有理素数，则必有 $p=2$ 或 $p\equiv 1(\bmod 4)$。

证明 由于在 G 中，$N(\pi)$ 是一个平方和，故有理素数 p 可以表示成两个有理整数的平方和，因此由第六章定理 6.7.1 即得 $p=2$ 或 $p\equiv 1(\bmod p)$。

定理 9.4.8 π 是 G 中的素数的充分必要条件是

(1) π 是 $1+\mathrm{i}$ 或其相伴数；

(2) $N(\pi)$ 是 $4m+1$ 形式的有理素数；

(3) π 是 $4m+3$ 形式的正有理素数或其相伴数。

证明 为了看出我们是如何找出 G 中的所有素数的，我们先证必要性。

设 π 是 G 中的素数，那么由通常整数中的唯一分解定理知 $N(\pi)$ 可分解成有限个有理素数的乘积：$N(\pi)=p_1p_2\cdots p_r$。又由引理 9.4.4 知 $\pi \mid N(\pi)=p_1p_2\cdots p_r$。由于 π 是 G 中的素数，因此由素数的定义就得出 π 必整除某一个有理素数 p，或等价的 $\pi \mid p$。因而又有 $N(\pi)\mid N(P)=p^2$，由此就得出 $N(\pi)=p$ 或 $N(\pi)=p^2$（$N(\pi)$ 不可能等于 1，否则就得出 π 是 G 中的单位数，这与 π 是 G 中的素数的假设矛盾）。

如果 $N(\pi)=p$，那么由引理 9.4.5 就得出 $p=2$ 或 $p\equiv 1(\bmod 4)$。而从 $p=2$ 易于得出 π 是 $1+\mathrm{i}$ 或其相伴数，因此这就得出条件(1) 或(2)。

如果 $N(\pi)=p^2$，那么由 $\pi \mid p$ 就得出 $p=\pi\alpha$，因而

$$p^2=N(p)=N(\pi)N(\alpha)=p^2N(\alpha)$$

由此得出 $N(\alpha)=1$，这就说明 α 是单位数，由此得出 π 是 p 的相伴数。

p 不可能等于 2，否则有 $N(\pi)=4$，由此易于得出 $\pi=2$ 或 $\pi=2\mathrm{i}$。但是在 G 中

$$2=(1+\mathrm{i})(1-\mathrm{i})$$

因此 2 不是 G 中的不可约元或素数，这与 π 是 G 中的素数的假设矛盾。

p 也不可能是形如 $4m+1$ 的有理素数，否则由引理 9.4.2 知必存在自然数

n,使得

$$p \mid n^2 + 1 = (n + \mathrm{i})(n - \mathrm{i})$$

由于 p 是 π 的相伴数,因而由 π 是 G 中素数就得出 p 是 G 中素数,因此必有 $p \mid n + \mathrm{i}$ 或 $p \mid n - \mathrm{i}$,由此得出

$$p^2 = N(p) \mid N(n + \mathrm{i}) = n^2 + 1 = p$$

或

$$p^2 = N(p) \mid N(n - \mathrm{i}) = n^2 + 1 = p$$

总之我们得出 $p^2 \mid p$,因而 $p = 1$,这与 p 是有理素数的假设矛盾。

综合以上论述就得出必有 π 是 p 的相伴数,而 p 是 $4m + 3$ 形式的正有理素数。这就是条件(3)。

下面证明充分性,如果条件(1),(2)成立,那么 $N(\pi)$ 必是通常整数中的素数,因此由引理 9.4.3 就得出 π 是 G 中的素数。

如果条件(3)成立,那么 π 是 p 的相伴数,并且 p 是形如 $4m + 3$ 的正有理素数。

我们证 π 一定是 G 中的不可约元。假设不然,则 $\pi = \alpha\beta$,其中 α 和 β 都不是单位数。因此

$$N(\pi) = N(\varepsilon p) = p^2 = N(\alpha)N(\beta)$$

由于 $N(\alpha)$ 既不能等于 1(否则 α 是单位数)又不能等于 p^2(否则 β 是单位数),同样 $N(\beta)$ 既不能等于 1 又不能等于 p^2,故只能有

$$N(\alpha) = N(p) = p$$

这表明 p 可以表示成两个有理整数的平方和,因此由第六章定理 6.7.1 即得 $p = 2$ 或 $p \equiv 1 \pmod 4$。而这与 p 是形如 $4m + 3$ 的正有理素数的条件相矛盾。

因此 π 一定是 G 中的不可约元,由于在 G 中,不可约元就是素数,所以 π 一定是 G 中的素数。这就证明了充分性。

至此为止,可以说,我们已经弄清了 G 中素数的基本性质。

下面我们再来看一个环。

定义 9.4.15 用 $k(\omega)$ 表示所有形如 $a + b\omega$ 的数的集合,其中 $\omega = \dfrac{-1 + \mathrm{i}\sqrt{3}}{2}$,$a$,$b$ 都是有理整数。

不难验证有

引理 9.4.6 $k(\omega)$ 是一个有单位元的整环。

有了对 G 的讨论作为基础。我们下面对 $k(\omega)$ 的讨论就可以比较简单,其主要目地是想让读者注意到 $k(\omega)$ 中的元素作为一个复数,一般的并不具有我们上面已讨论过的复整数的形式,因为 $a + b\omega = a - \dfrac{b}{2} + \dfrac{b}{2}\mathrm{i}\sqrt{3}$ 中的 $a - \dfrac{b}{2}$ 和

$\frac{b}{2}$ 在一般情况下都不是整数。既然如此，那为什么我们还把 $k(\omega)$ 看成整数的一种推广呢？这是由于 $k(\omega)$ 中的任意元素 $a + b\omega$，一定满足方程

$$x^2 - (2a - b)x + a^2 - ab + b^2 = 0$$

因而 $a + b\omega$ 一定是一个代数整数。所以从代数数的角度看来，$k(\omega)$ 仍是整数的一种推广。

在上面我们已经看到，从复数的模可以导出 G 中的模。如果模仿这一手段，我们也可以从复数的模导出 $k(\omega)$ 中的模。通过类比，这个模在数值上应该等于

$$\left(a - \frac{b}{2}\right)^2 + \left(\frac{\sqrt{3}b}{2}\right)^2 = a^2 - ab + b^2 = \left(a - \frac{b}{2}\right)^2 + \frac{3}{4}b^2$$

我们就以此作为 $k(\omega)$ 中的模。

定义 9.4.16 任给 $\alpha = a + b\omega \in k(\omega)$，定义 α 的模为 $a^2 - ab + b^2$，记为 $N(\alpha)$。

容易验证，$k(\omega)$ 中的模有和 G 中的模类似的性质，即引理 9.4.1 在 $k(\omega)$ 中也成立。

引理 9.4.7 在 $k(\omega)$ 中，模有如下性质：

(1) $N(\alpha)$ 是一个整数；

(2) $N(\alpha) = \alpha\bar{\alpha}$；

(3) $N(\alpha\beta) = N(\alpha)N(\beta)$；

(4) $N(\alpha) = 0$ 的充分必要条件是 $\alpha = 0$；

(5) $N(\alpha) = 1$ 的充分必要条件是 α 是单位数；

(6) α, β 是相伴数的充分必要条件是 $N(\alpha) = N(\beta)$。

下面我们证明，在 $k(\omega)$ 中也成立第二带余数除法。

定理 9.4.9 在 $k(\omega)$ 中成立第二带余数除法，即对任意 $\alpha, \beta \in k(\omega)$，$\alpha \neq 0$，一定存在 $\eta, \gamma \in k(\omega)$，使得

$$\beta = \eta\alpha + \gamma, 0 \leqslant N(\gamma) < N(\alpha)$$

证明 设 $\frac{\beta}{\alpha} = r + s\mathrm{i}$，其中 r, s 都是有理数。设 u, v 分别是距离 r, s 最近的有理整数。那么显然就有

$$|u - r| \leqslant \frac{1}{2}, |v - s| \leqslant \frac{1}{2}$$

现在令 $\eta = u + v\mathrm{i}$，$\gamma = \beta - \alpha\eta$，因此 $\beta = \eta\alpha + \gamma$，则

$$\begin{aligned} N(\gamma) = N(\beta - \alpha\eta) = N(\alpha)N\left(\frac{\beta}{\alpha} - \eta\right) = \\ N(\alpha)N(r + s\mathrm{i} - u - v\mathrm{i}) = \\ N(\alpha)N((r - u) + (s - v)\mathrm{i}) = \end{aligned}$$

$$
\begin{aligned}
&((r-u)^2-(r-u)(s-v)+(s-v)^2)N(\alpha)\leqslant\\
&(|r-u|^2+|r-u||s-v|+|s-v|^2)N(\alpha)\leqslant\\
&\left(\left(\frac{1}{2}\right)^2+\left(\frac{1}{2}\right)+\left(\frac{1}{2}\right)+\left(\frac{1}{2}\right)^2\right)N(\alpha)\leqslant\frac{3}{4}N(\alpha)<N(\alpha)
\end{aligned}
$$

这就证明了定理。

由引理9.4.7和定理9.4.9完全和对 G 所进行的讨论类似，我们可以证明：

定理 9.4.10 $k(\omega)$ 既是可分解整环同时又是欧几里得环，因而在 $k(\omega)$ 中，定理9.4.1、定理9.4.6、定理9.4.7、引理9.4.3和引理9.4.4都成立。

于是与 G 类似，为了掌握 $k(\omega)$ 的基本算术性质，剩下的只是确定 $k(\omega)$ 中的单位数和素数是什么了。

与 G 类似，第一个问题不难解决，容易证明：

引理 9.4.8 $k(\omega)$ 共有6个单位数，它们是 $\pm 1,\ \pm\omega,\ \pm\omega^2$。

为解决第二个问题，我们，需要以下引理：

引理 9.4.9 设 p 是有理奇素数，那么 $\left(\frac{-3}{p}\right)=1$ 的充分必要条件是 $p\equiv 1 \pmod 3$。

证明 由于 p 是有理奇素数，因此

$$
\begin{aligned}
\left(\frac{-3}{p}\right)&=\left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)=(-1)^{\frac{p-1}{2}}\left(\frac{3}{p}\right)=\left(\frac{3}{p}\right)=\\
&(-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}}(-1)^{\frac{3-1}{2}}\left(\frac{p}{3}\right)=\\
&(-1)^{p-1}\left(\frac{p}{3}\right)=\left(\frac{p}{3}\right)
\end{aligned}
$$

由此得出 $\left(\frac{-3}{p}\right)=\left(\frac{1}{3}\right)$ 的充分必要条件是 $p\equiv 1 \pmod 3$，$\left(\frac{-3}{p}\right)=\left(\frac{2}{3}\right)$ 的充分必要条件是 $p\equiv 2 \pmod 3$。而由于 $\left(\frac{1}{3}\right)=1$，$\left(\frac{2}{3}\right)=(-1)^{\frac{3^2-1}{8}}=-1$，$\left(\frac{-3}{p}\right)=1$ 的充分必要条件就是 $p=1 \pmod 3$。

引理 9.4.10 $1-\omega$ 是 $k(\omega)$ 中的素数。

证明 $N(1-\omega)=N\left(1-\left(\frac{-1}{2}+\frac{\mathrm{i}\sqrt{3}}{2}\right)\right)=N\left(\frac{3}{2}-\frac{\mathrm{i}\sqrt{3}}{2}\right)=$

$$
\left(\frac{3}{2}\right)^2+\left(\frac{\sqrt{3}}{2}\right)^2=3
$$

是有理素数，因此由引理9.4.3即得 $1-\omega$ 是 $k(\omega)$ 中的素数。

定理 9.4.11 π 是 $k(\omega)$ 中的素数的充分必要条件是：

(1) π 是 $1-\omega$ 或其相伴数；

(2) $N(\pi)$ 是 $3m+1$ 形式的有理素数；

(3) π 是 $3m+2$ 形式的正有理素数或其相伴数；

证明 设 π 是 $k(\omega)$ 中的素数。那么由通常整数中的唯一分解定理知 $N(\pi)$ 可分解成有限个有理素数的乘积

$$N(\pi) = p_1p_2\cdots p_r$$

又由引理9.4.4知 $\pi \mid N(\pi) = p_1p_2\cdots p_r$。由于 π 是 $k(\omega)$ 中的素数，因此由素数的定义就得出 π 必整除某一个有理素数 p，或等价的 $\pi \mid p$。因而又有 $N(\pi) \mid N(p) = p^2$，由此就得出 $N(\pi) = p$ 或 $N(\pi) = p^2$（$N(\pi)$ 不可能等于1，否则就得出 π 是 G 中的单位数，这与 π 是 G 中的素数的假设矛盾）。

现在以3为模，分成三种情况讨论。

(1) $p \equiv 3 \pmod 3$。这时 $p = 3 = -\omega^2(1-\omega)^2$，由引理9.4.8、引理9.4.10知 ω 是 $k(\omega)$ 中的单位数，$1-\omega$ 是 $k(\omega)$ 中的素数。因此 p 的素因子分解式中只含有一个素因子。因而由 $\pi \mid p$，π 是 $k(\omega)$ 中的素数就得出条件(1)。反之如果条件(1)成立，那么由引理9.4.10知 $1-\omega$ 是 $k(\omega)$ 中的素数。

(2) $p \equiv 1 \pmod 3$。那么 $p \neq 2$，因而 p 是有理奇素数，因此由引理9.4.9知 $\left(\frac{-3}{p}\right) = 1$。这就是说同余式方程 $x^2 \equiv -3 \pmod p$ 有解，因此存在自然数 n 使 $p \mid n^2+3$，或者 $p \mid (n+\mathrm{i}\sqrt{3})(n-\mathrm{i}\sqrt{3}) = (n+1+2\omega)(n-1-2\omega)$。我们证 p 不能是 $k(\omega)$ 中的素数，否则将由 $p \mid (n+\mathrm{i}\sqrt{3})(n-\mathrm{i}\sqrt{3}) = (n+1+2\omega)\cdot(n-1-2\omega)$ 得出 $p \mid n+1+2\omega$ 或 $p \mid n-1-2\omega$，而这显然不可能。这样一来，$p = \alpha\beta$，其中 α 和 β 都不是单位数，因而必有 $N(\alpha) = N(\beta) = p$，由此得出 $\pi \mid \alpha$ 或 $\pi \mid \beta$，而 $N(\pi) = p \equiv 1 \pmod 3$。这就得出条件(2)。反之，如果条件(2)成立，那么由引理9.4.10知一定是 $k(\omega)$ 中的素数。

(3) $p \equiv 2 \pmod 3$，那么

$$4N(\pi) = (2a-b)^2+3b^2 \equiv (2a-b)^2 \pmod 3 \equiv (2a+b)^2 \pmod 3 \equiv 0,1 \pmod 3$$

因此 $N(\pi) \equiv 0,1 \pmod 3$，这说明 $N(\pi) \neq p$，因而必有 $N(\pi) = p^2 = N(p)$。这就 π 是 p 说是的相伴数，故我们得出条件(3)。反之如果条件(3)成立，我们就有 $N(\pi) = N(p) = p^2$。设 $\pi = \alpha\beta$，则 $N(\alpha) \mid N(\pi) = p^2$，但是由于在这种情况下（即 $p \equiv 2 \pmod 3$ 时），上面已证，p 不可能是 $k(\omega)$ 中任何数的模，故必有 $N(\alpha) = 1$ 或 $N(\alpha) = p^2$。由此得出 α 是单位数或 π，因而 β 是 π 或单位数，这就证明了 π 一定是素数。

最后我们再来看一个集合 $Z[\sqrt{-5}]$，它是由所有形如 $a+b\sqrt{-5}$ 的数组成的，其中 a,b 都是有理整数。不难证明 $Z[\sqrt{-5}]$ 是一个有单位元的整环。

看这个环的目的是好比我们去动物园一样，可以看到各种动物。这个环具有许多和我们以前见过的环不一样的性质，初次见到这些性质，是很令人吃惊的，而且有些性质如果没有一个具体的例子，也是不太好凭空想象的。而既然诸

位读者都是对整数有些兴趣的，就应该也见识见识原来世界上还有这样的东西，也算是读万卷书，行万里路，增加了见识。

首先，类似于 G 和 $k(\omega)$，从复数的模可以诱导出 $Z[\sqrt{-5}]$ 的模，对任意 $\alpha=a+b\sqrt{-5}\in Z[\sqrt{-5}]$，$N(\alpha)=a^2+5b^2$，由于这些模都是从复数模诱导出来的，因此它们都具有引理 9.4.1 中所列举的几条性质。

我们依次证明下列命题或性质以观赏 $Z[\sqrt{-5}]$ 的奇特之处。

性质 1 $Z[\sqrt{-5}]$ 的单位元是 1 和 -1。

性质 2 $3,2+\sqrt{-5},2-\sqrt{-5}$ 都是 $Z[\sqrt{-5}]$ 中的不可约元。

证明 由于 $N(3)=N(2-\sqrt{-5})=N(2+\sqrt{-5})=9$，如果 $\pi=\alpha\beta$，这里 π 表示 $3,2+\sqrt{-5},2-\sqrt{-5}$ 中的任何一个数。那么由于 3 不可能是 $Z[\sqrt{-5}]$ 中任何数的模，所以由 $N(\alpha)N(\beta)=N(\pi)=9$ 只能得出 $N(\alpha)=1$ 或 $N(\alpha)=9$，因而 $N(\beta)=9$ 或 $N(\beta)=1$。因而只可能 α 是单位数，β 与 π 相伴或 α 与 π 相伴，β 是单位数。这就证明了 π 是不可约元。

性质 3 $Z[\sqrt{-5}]$ 不是唯一分解环。

例 9.4.1 $9=3\cdot3=(2+\sqrt{-5})(2-\sqrt{-5})$ 是两个不同的分解式。

性质 4 $Z[\sqrt{-5}]$ 中的不可约元不一定是素数。

例 9.4.2 $3\mid(2+\sqrt{-5})(2-\sqrt{-5})$，但是 $3\nmid 2\pm\sqrt{5}$，因此 3 不是素数。类似可证 $2\pm\sqrt{5}$ 也不是素数。

性质 5 在 $Z[\sqrt{-5}]$ 中，最大公因数不一定存在。

证明 我们证明 9 和 $3(2+\sqrt{-5})$ 没有最大公因数。假设 $\Delta=a+b\sqrt{-5}$ 是它们的最大公因数。其中 a,b 都是有理整数，那么由 3 和 $2+\sqrt{-5}$ 都是他们的公因数，因此按照最大公因数的定义就必有

$$3\mid\Delta,2+\sqrt{-5}\mid\Delta$$

由 $3\mid\Delta$ 得出 $\Delta=3(c+d\sqrt{-5})$，其中 c,d 都是有理整数。由 $\Delta\mid9$ 得出 $c+d\sqrt{-5}\mid3$。由于在性质 2 中已证 3 是不可约数，因此必有 $c+d\sqrt{-5}=\pm1$ 或 ±3。因此 $\Delta=\pm3$ 或 ±9。但是当 $\Delta=\pm3$ 时，$2+\sqrt{-5}\nmid\Delta$，当 $\Delta=\pm9$ 时，$3(2+\sqrt{-5})\nmid\Delta$。这就证明了 9 和 $3(2+\sqrt{-5})$ 没有最大公因数。两个数的最大公因数尚且可能不存在，一般的情况就更不用说了。既然最大公因数可能不存在，那有关最大公因数的种种公式在最大公因数根本不存在时当然就更成了废话。

性质 6 在 $Z\sqrt{-5}$ 中，最小公倍数不一定存在。

证明 我们证明 9 和 $3(2+\sqrt{-5})$ 没有最小公倍数。由定理 9.4.1(11) 知如果 9 和 $3(2+\sqrt{-5})$ 的最小公倍数存在，则它们的最大公约数也一定存在。然而在性质(5)中，我们已证明 9 和 $3(2+\sqrt{-5})$ 不存在最大公约数。因此它们不可能有最小公倍数。与最大公约数的情况类似，既然两个数的最小公倍数尚且

可能不存在，一般的情况就更不用说了。在根本不存在最小公倍数的情况下，自然也谈不到涉及这一概念的公式之类。

性质 7 $Z[\sqrt{-5}]$ 不可能是欧几里得环。

证明 由定理9.4.6知在欧几里得环中最大公因数一定存在，而上面在性质5中已经证明在 $Z[\sqrt{-5}]$ 中最大公因数可能不存在，因此 $Z[\sqrt{-5}]$ 不可能是欧几里得环。

当然我们直接用 $Z[\sqrt{-5}]$ 的模也可以证明 $Z[\sqrt{-5}]$ 不是欧几里得环。但是这样去证就会引出另一个问题，那就是你对这个模证明欧几里得算法不成立，那是否会存在一个你不知道的模，在那个模下，欧几里得算法可以成立呢？这是一个不好回答的问题。而上面的证明说明，不管你怎样定义 $Z[\sqrt{-5}]$ 中的模，只要那个模具有引理9.4.1中的几条性质，那么对这个模就不可能成立欧几里得算法。

由此问题又可以引发出另一个比较细致的问题，那就是是否存在不是欧几里得环，但是最大公因数仍一定存在的环？老实说，这样的例子作者也没有见到过，如果有的读者有兴趣，可以去探讨一下，如果能回答这一问题，也是有兴趣的。

9.5 $n=3$ 时的费马问题

在9.4中，我们已经游览了一个整数推广的小型花园。不过在游览之余，有些读者可能会感到，你花了这么多篇幅建立了各种复整数的基本性质，究竟有什么用呢？确实，大多数普通人对科学也会发生这种感想，如果科学研究的成果不会对他们的生活产生影响，大概大多数人都会对其采取敬而远之的态度吧！

本书的读者多少都对整数有些兴趣，因此，如果整数的推广不能对解决我们一直很熟悉的整数中的问题有作用，大概也就会感到对这种推广没什么兴趣了，毕竟离我们距离最近的还是我们已经熟悉的普通整数。在这一节中，我们将表明，推广的整数确实有助于解决普通整数中的问题。事实上，在历史上，讨论上一节的内容的动机正是为了解决普通整数中的一个很著名的问题，即费马问题。

在这一节中，我们要讨论的广义整数是所有形如 $a+b\sqrt{-3}$ 的数，其中 a，b 都是普通的整数。我们用 $Z[\sqrt{-3}]$ 表示所有这种数的集合。容易验证 $Z[\sqrt{-3}]$ 是一个有单位元的整环。从复数的模可以诱导出 $Z[\sqrt{-3}]$ 的模：对任意 $\alpha=a+b\sqrt{-3}$，$N(\alpha)=a^2+3b^2$。由此可确定其单位数为 ± 1。（注意：环中的单位元和有模的环中的单位数不是一回事）

作为集合，$Z[\sqrt{-3}] \subset k(\omega)$，不过这两个环的性质却差别很大，最主要的区别是 $k(\omega)$ 是欧几里得环，因此有许多好的性质。而这个 $Z[\sqrt{-3}]$ 却类似于 $Z[\sqrt{-5}]$，有点怪怪的。你只要注意到在 $Z[\sqrt{-3}]$ 中，2 不可能是任何数的模，然后把上一节中对 $Z[\sqrt{-5}]$ 中讨论时所用的 $9, 3, 2+\sqrt{-5}$ 和 $2-\sqrt{-5}$ 换成 $4, 2, 1+\sqrt{-3}$ 和 $1-\sqrt{-3}$，就可以像上一节那样一模一样地证明 $Z[\sqrt{-3}]$ 具有像上一节中 $Z[\sqrt{-5}]$ 的那些性质。

不过，尽管如此，在这一节中，我们还是要证明 $Z[\sqrt{-3}]$ 中的一种特殊元素，有类似于唯一分解式的性质，并利用此性质来解决 $n=3$ 时的费马问题。

引理 9.5.1 两个形如 a^2+3b^2 的整数的乘积仍是一个形如 a^2+3b^2 整数。

证明 设 $\alpha = a+b\sqrt{-3}, \beta = c+d\sqrt{-3}$，那么由 $N(\alpha)N(\beta) = N(\alpha\beta)$ 就得出

$$(a^2+3b^2)(c^2+3d^2) = (ac-3bd)^2 + 3(ad+bc)^2$$

这就证明了引理。

引理 9.5.2 设 N 是形如 a^2+3b^2 的整数，那么

(1) 当 a, b 的奇偶性相反时，N 是奇数；

(2) 当 a, b 的奇偶性相同时，$4 \mid N$，并且 $\dfrac{N}{4}$ 仍是形如 a^2+3b^2 的整数；

(3) 如果 $2 \mid N$，那么 $4 \mid N$，并且 $\dfrac{N}{4}$ 仍是形如 a^2+3b^2 的整数。

证明 (1) 显然。

(2) 当 a, b 都是偶数时，引理也显然成立。以下设 a, b 都是奇数。

这时可设 $a = 4m \pm 1, b = 4n \pm 1$，其中 a, b 中的正负号可以根据需要自由选择。因此 $a+b$ 或者 $a-b$ 可以被 4 整除。

如果 $4 \mid a+b$，那么由于 $a-3b = a+b-4b$ 可被 4 整除，所以 $4(a^2+3b^2) = (a-3b)^2 + 3(a+b)^2$ 可被 4^2 整除，这就得出 $4 \mid N$，并且 $\dfrac{N}{4}$ 仍是形如 a^2+3b^2 的整数；如果 $4 \mid a-b$，那么由于 $a+3b = a-b+4b$ 可被 4 整除，所以 $4(a^2+3b^2) = (a+3b)^2 + 3(a-b)^2$ 可被 4^2 整除，这就得出 $4 \mid N$，并且 $\dfrac{N}{4}$ 仍是形如 a^2+3b^2 的整数。

(3) 由于 $2 \mid N$，因此由 (1) 得出 a, b 的奇偶性相同，因而再由 (2) 就得出 (3)。

引理 9.5.3 设 N 是形如 a^2+3b^2 的整数，如果 N 可被一个形如 a^2+3b^2 的素数 p 整除，那么 $\dfrac{N}{p}$ 仍是形如 a^2+3b^2 的一个整数。

证明 设 $p = c^2+3d^2$，那么由

$$(bc-ad)(bc+ad) = b^2(c^2+3d^2) - d^2(a^2+3b^2) = b^2p - d^2N$$

得出
$$p \mid (bc-ad)(bc+ad)$$
由于 p 是素数,因此 $p \mid bc-ad$ 或 $p \mid bc+ad$。再由
$$pN=(c^2+3d^2)(a^2+3b^2)=(ac\mp 3bd)^2+3(bc\pm ad)^2$$
可知当 $p \mid bc-ad$ 时,$p \mid ac+3bd$,当 $p \mid bc+ad$ 时,$p \mid ac-3bd$,由此就得出
$$\frac{N}{p}=\frac{pN}{p^2}=\left(\frac{ac\mp 3bd}{p}\right)^2+3\left(\frac{bc\pm ad}{p}\right)^2$$
因而$\frac{N}{p}$仍是形如 a^2+3b^2 的整数。

引理 9.5.4 设 N 是形如 a^2+3b^2 的整数。如果 N 有一个不是这种形式的奇因数 h,那么$\frac{N}{h}$也有一个不是这种形式的奇因数。

证明 设 $N=hy$,如果 y 是偶数,那么由引理 9.5.2(3) 可知 N 可被 4 整除,且 $h\frac{y}{4}$ 仍是一个形如 a^2+3b^2 的整数,如果$\frac{y}{4}$仍是偶数,那么同理$\frac{N}{4}$是形如 a^2+3b^2 的整数,可被 4 整除,因而$\frac{N}{4^2}$仍是一个形如 a^2+3b^2 的整数,反复进行这一程序就得出,一定存在一个自然数 k,使得$\frac{y}{4^k}$是异于 1 的奇数(否则由引理9.5.2 得出 $h=\frac{N}{4^k}$ 也具有这种形式,与假设不符)。因此 $y=p_1p_2\cdots p_n$,其中 p_i 或者是 4,或者是一个奇素数。如果在 y 的上述分解式中,所有的奇素数都具有形式 a^2+3b^2,那么由引理 9.5.1 ~ 引理 9.5.3 就得出
$$h=\frac{1}{p_1}\left(\frac{1}{p_2}\left(\cdots\left(\frac{m}{p_n}\right)\right)\right)$$
仍是一个形如 a^2+3b^2 的整数,而这与假设不符,因此在 y 的分解式中,必有一个奇因数不具有这种形式。

引理 9.5.5 设 N 是形如 a^2+3b^2 的整数,并且 a,b 互素,则 N 的奇因数仍是一个形如 a^2+3b^2 的整数。

证明 设 x 是 N 的任意正的奇因数。

用 a 去除以 x,由带余数除法 $a=qx+r,0\leqslant r<x$,由于 x 是奇数,因此或者 $r<\frac{x}{2}$ 或者 $r>\frac{x}{2}$。当 $r<\frac{x}{2}$ 时,令 $m=q$,这时 $|r|=r<\frac{x}{2}$;当 $r>\frac{x}{2}$ 时,$a=(q+1)x+r-x$,这时 $|r-x|=x-r<\frac{x}{2}$。我们令 $m=q+1$,总之,我们可以把 a 写成 $mx+c$ 的形式,其中 $|c|<\frac{x}{2}$。

再用 $-a$ 去除以 x,利用上面已证的结果,可把 $-a$ 写成 $-mx+c$(这里的

m 与前面的 m 不一定代表同一个数字，只代表一种形式）的形式，其中 $|c|<\frac{x}{2}$，因此我们又可以把 a 写成 $mx-c$ 的形式，其中 $|c|<\frac{x}{2}$（在这两种形式中，m 和 c 不一定代表同样的数字，只代表 a 可以写成的形式）。

因此我们可设 $a=mx\pm c, b=nx\pm d, |c|<\frac{x}{2}, |d|<\frac{x}{2}$。因而 $c^2+3b^2<x^2$。

由于

$$c^2+3d^2=(a-mx)^2+3(b-nx)^2\equiv a^2+3b^2 \pmod x \equiv 0 \pmod x$$

（因为 x 是 $N=a^2+3b^2$ 的奇因数）所以 c^2+3d^2 可被 x 整除。因而可设 $c^2+3d^2=xy$，并且 $y<x$（由于 $c^2+3d^2<x^2$）。从 $c^2+3d^2=xy$ 两边约去 $(c,d)^2$ 后，我们得到 $e^2+3f^2=xz$，现在 e,f 已经是互素的了。如果 x 不具有 a^2+3b^2 的形式，那么由引理 9.5.4 知 z 就有一个奇因数 x_1 也不具有 a^2+3b^2 的形式。而 $x_1<x$，如此反复进行下去，就得出无穷多个正奇数 $x_1,x_2,\cdots,x_n,\cdots$ 使得 $0<\cdots<x_n<\cdots<x_2<x_1<x$，这显然是一个矛盾，所得的矛盾就证明了 x 一定具有 a^2+3b^2 的形式。

引理 9.5.6 N 是一个具有 a^2+3b^2 形式的正整数的充分必要条件是 $\frac{N}{M^2}$ 不含有形如 $3n+2$ 的素因数，其中 M 是一个整数使得 $\frac{N}{M^2}$ 中不含任何平方因数。

证明 先证必要性。

$\frac{N}{M^2}$ 显然仍具有 a^2+3b^2 的形式，并且这时 a,b 是互素的。因此不妨设 $N=a^2+3b^2$，并且 a,b 是互素的。如果 $N\equiv 2 \pmod 3$，那么由 $N=a^2+3b^2$ 就得出 $a^2\equiv N\equiv 2 \pmod 3$，因此 $a\equiv 1 \pmod 3$ 或 $a\equiv 2 \pmod 3$，但是无论哪种情况都得出 $a^2\equiv 1 \pmod 3$，这是一个矛盾，所得的矛盾说明 $N\not\equiv 2 \pmod 3$，由 a,b 互素又得出 $N\not\equiv 0 \pmod 3$，因此只能有 $N\equiv 1 \pmod 3$，并且 $N>3$。这样由引理 9.5.5 就得出 N 不可能含有形如 $3n+2$ 的素因数。

充分性就是要证明如果 $\frac{N}{M^2}$ 不含有形如 $3n+2$ 的素因数，则 $\frac{N}{M^2}$ 必具有 a^2+3b^2 的形式。$\frac{N}{M^2}$ 的素因数 p 都是单的，由假设 $p\neq 2$，由于 $3=0^2+3\cdot 1^2$ 已具有 a^2+3b^2 的形式。因此我们只须对大于 3 的素数 p 证明 p 必具有 a^2+3b^2 的形式，那么由引理 9.5.1 即可知道 $\frac{N}{M^2}$ 也具有这种形式。

当 $p>3$ 时，由于 p 是素数，故 $p\not\equiv 0 \pmod 3$，又由假设 $p\not\equiv 2 \pmod 3$，因

此只能有 $p\equiv 1(\bmod 3)$,或 $p=3n+1$。这时由费马小定理知对任何整数 a 成立

$$a^{p-1}\equiv 1(\bmod p)\text{ 或 }a^{3n}\equiv 1(\bmod p)$$

令 $a=1,2,3,\cdots,p-1$ 就得出 $p-1$ 个同余式,再由这 $p-1$ 个同余式就得出

$$p\mid 1^{3n}-1,p\mid 2^{3n}-1,p\mid 3^{3n}-1,\cdots,p\mid (p-1)^{3n}-1$$

因而我们又可得出 $p-2$ 个整除关系如下

$$p\mid 2^{3n}-1^{3n},p\mid 3^{3n}-2^{3n},\cdots,p\mid (p-1)^{3n}-(p-)^{3n}$$

上面的每一个整除关系的的右边都具有形式

$$a^{3n}-b^{3n}=(a^n-b^n)(a^{2n}+a^nb^n+b^{2n})$$

由于 a,b 是相邻的整数,因此 a,b 必是一奇一偶,因而 a^n,b^n 也必是一奇一偶。这就是说,上面式子中右边的第二个括弧必可写成

$$A^2+A(2B)+(2B)^2=(A+B)^2+3B^2$$

的形式,因而上面式子中右边的第二个括弧都具有 a^2+3b^2 的形式。而且由

$(A+B,B)=(A,B)=(a^n,b^n)=(a,b)=1$(由于 a,b 是相邻的整数)

可知,可设 a,b 是互素的。

在上面的 $p-2$ 个整除关系中,必有某一个关系使得 p 整除第二个括弧。否则我们将得出

$$p\mid 2^n-1,p\mid 3^n-1,\cdots,p\mid (p-1)^n-1$$

由此又得出

$$p\mid 2^n-1,p\mid 3^n-2^n,\cdots,p\mid (p-1)^n-(p-2)^n$$

现在我们从 $1^n,2^n,\cdots,(p-1)^n$ 开始,构造以下的差分表

$$\begin{array}{ccccc} 1^n & 2^n & 3^n\ \cdots\ \cdots & (p-1)^n \\ \Delta(2) & \Delta(3) & \cdots\ \cdots & \Delta(p-1) \\ & \Delta^2(3) & \Delta^2(4)\cdots\Delta^2(p-1) & \\ & & \cdots\ \cdots & \\ & & \Delta^n(p-1) & \end{array}$$

其中 $\Delta(x)=x^n-x^{n-1},\Delta^2(x)=\Delta(\Delta(x)),\cdots,\Delta^n(x)=\Delta(\Delta^{n-1}(x))$,由此可知:

(1) p 整除上表的第二行;

(2) 上表中,每一行的下一行中的数,如果看成 x 的多项式,它的次数都要比上一行低一次;

(3) 上表中,每一行的下一行中的数,都是其上一行中相邻的两个数的差;

由(1)和(3)又得出:

(4) p 整除上表的第二行,第三行,$\cdots$,乃至第二行以后的任意一行;

由(2)得出：

(5) 上表中的第 n 行是一个常数。

至于这个常数到底是多少?我们可以通过观察具体的差分表而归纳出来就是 $n!$。(我们将在下一章中插值多项式一节中严格地证明这一结果)

因而我们就得出 $p \mid n!$。但是由于 p 是一个素数，所以由此就得出，$p \mid k$，其中 k 是某个小于或等于 n 的整数，然而由 $p = 3n + 1$ 知 $k \leqslant n < p$，因此这是不可能的。所得的矛盾说明在 $p - 2$ 个整除关系

$$p \mid 2^{3n} - 1^{3n}, p \mid 3^{3n} - 2^{3n}, \cdots, p \mid (p-1)^{3n} - (p-2)^{3n}$$

中，必有某一个使得 p 整除 $a^{3n} - b^{3n} = (a^n - b^n)(a^{2n} + a^n b^n + b^{2n})$ 中右边第二个括弧，因而 p 是一个形如 $a^2 + 3b^2$ 的数的素因数，其中 a, b 是互素的。这样，由引理 9.5.5 就得出 p 本身也具有 $a^2 + 3b^2$ 的形式。这就证明了充分性。

以上几个引理的意义在于在一定条件下在有理整数的范围内弄清了具有 $N = a^2 + 3b^2$ 形式的整数的因数，基本的结果是，如果 a, b 是互素的，那么 N 只可能有两种因数。其偶因数只能是 4，其奇因数必仍具有 $a^2 + 3b^2$ 的形式。这里面还有一些细微的性质在有理整数范围内是看不出来的，而只有在 $Z[\sqrt{-3}]$ 中才能表现出来。我们可把上面的几个引理几乎是逐字逐句地“翻译”成 $Z[\sqrt{-3}]$ 中的引理，这样，你就能看出同样的事实在有理整数中和在 $Z[\sqrt{-3}]$ 中表述上的差别了。

引理 9.5.7 设 a, b 是互素的且 $N = a^2 + 3b^2$ 是偶数，那么

(1) $4 \mid a + b$ 或 $4 \mid a - b$；

(2) $4 \mid a + b$ 的充分必要条件是 $a + b\sqrt{-3} = (1 - \sqrt{-3})(u + v\sqrt{-3})$，其中 u, v 是互素的有理整数；

(3) $4 \mid a - b$ 的充分必要条件是 $a + b\sqrt{-3} = (1 + \sqrt{-3})(u + v\sqrt{-3})$，其中 u, v 是互素的有理整数；

(4) $N = a^2 + 3b^2 = 4(u^2 + 3v^2)$。

证明 (1) 由于 N 是偶数，因此 a, b 必具有相同的奇偶性，而由于 a, b 是互素的，因此 a, b 必定同时是奇数。因而或者 $4 \mid a + b$，或者 $4 \mid a - b$(考虑模 4 下 a, b 仅可能具有的两种形式及其搭配)。

(2) 如果 $4 \mid a + b$，则

$$4 \mid (a + b) - 4b = a - 3b$$

因而

$$4(a^2 + 3b^2) = (a - 3b)^2 + 3(a + b)^2$$

可被 4^2 整除。这就说明

$$\frac{a^2 + 3b^2}{4} = \frac{4(a^2 + 3b^2)}{4^2} = \frac{(a - 3b)^2 + 3(a + b)^2}{4^2} = u^2 + 3v^2$$

其中 $u=\frac{a-3b}{4},v=\frac{a+b}{4}$ 都是有理整数。由此得出

$$u+v\sqrt{-3}=\frac{a-3b}{4}+\frac{a+b}{4}\sqrt{-3}=(a+b\sqrt{-3})\left(\frac{1+\sqrt{-3}}{4}\right)$$

因而
$$a+b\sqrt{-3}=(1-\sqrt{-3})(u+v\sqrt{-3})$$

反之,如果

$$a+b\sqrt{-3}=(1-\sqrt{-3})(u+v\sqrt{-3})$$

那么

$$u+v\sqrt{-3}=\frac{a-3b}{4}+\frac{a+b}{4}\sqrt{-3}=(a+b\sqrt{-3})\left(\frac{1+\sqrt{-3}}{4}\right)$$

因而 $u=\frac{a-3b}{4},v=\frac{a+b}{4}$,这就得出 $4\mid a-3b+4b=a+b$。因而 $4\mid a+b$ 的充分必要条件是 $a+b\sqrt{-3}=(1-\sqrt{-3})(u+v\sqrt{-3})$,其中 u,v 都是有理整数。

由 $u=\frac{a-3b}{4},v=\frac{a+b}{4}$ 容易得出 $a=u+3v,b=u-v$,因此由 a,b 是互素的显然就得出 u,v 是互素的。

(3) 同理可证,$4\mid a-b$ 的充分必要条件是

$$a+b\sqrt{-3}=(1+\sqrt{-3})(u+v\sqrt{-3})$$

其中 u,v 是互素的有理整数。

(4) 显然有 $N=a^2+3b^2=4(u^2+3v^2)$。

引理 9.5.8 设 a,b 是互素的且 $N=a^2+3b^2$ 可被奇素数 P 整除,那么

(1) $P=p^2+3q^2$,其中 p,q 都是正整数;

(2) $P\mid pb+aq$ 或 $P\mid pb-aq$;

(3) $P\mid pb+aq$ 的充分必要条件是 $a+b\sqrt{-3}=(p-q\sqrt{-3})(u+v\sqrt{-3})$,其中 u,v 是互素的有理整数;

(4) $P\mid pb-aq$ 的充分必要条件是 $a+b\sqrt{-3}=(p+q\sqrt{-3})(u+v\sqrt{-3})$,其中 u,v 是互素的有理整数;

(5) $N=a^2+3b^2=P(u^2+3v^2)$。

证明 (1) 由引理 9.5.5 即得。

(2) 由 $P\mid N$ 和

$$(pb-aq)(pb+aq)=b^2(p^2+3q^2)-q^2(a^2+3b^2)=b^2P-d^2N$$

即可得出
$$P\mid(pb-aq)(pb+aq)$$

由于 P 是素数,所以必有 $P\mid pb+aq$ 或 $P\mid pb-aq$。

(3) 如果 $P\mid pb+aq$,则

$$P(a^2+3b^2)=(pa-3qb)^2+3(pb+aq)^2$$

可被 P^2 整除，因此

$$\frac{a^2+3b^2}{P}=\frac{P(a^2+3b^2)}{P^2}=u^2+3v^2$$

其中 $u=\dfrac{pa-3qb}{P}$，$v=\dfrac{pb+aq}{P}$ 都是有理整数。这也就是

$$u+v\sqrt{-3}=\frac{(p+q\sqrt{-3})(a+b\sqrt{-3})}{P}$$

由此就得出

$$a+b\sqrt{-3}=(p-q\sqrt{-3})(u+v\sqrt{-3})$$

其中 u,v 都是有理整数。

由 $u=\dfrac{pa-3qb}{P}$，$v=\dfrac{pb+aq}{P}$ 得出 $a=pu+3qv$，$b=-qu+pv$，因此由 a,b 是互素的显然就得出 u,v 是互素的。

(4) 同理可证 $P\mid pb-aq$ 的充分必要条件是

$$a+b\sqrt{-3}=(p+q\sqrt{-3})(u+v\sqrt{-3})$$

其中 u,v 是互素的有理整数。

(5) 显然有 $N=a^2+3b^2=P(u^2+3v^2)$。

引理 9.5.9 设 a,b 互素，那么

$$a+b\sqrt{-3}=(p_1+\varepsilon_1q_1\sqrt{-3})(p_2+\varepsilon_2q_2\sqrt{-3})\cdots(p_n+\varepsilon_nq_n\sqrt{-3})$$

其中 p_i,q_i 都是有理整数，ε_i 等于 1 或 -1，并且 $p_i^2+3q_i^2$ 或者是 4 或者是一个奇素数。或

$$a+b\sqrt{-3}=\pm(p_1+\varepsilon_1q_1\sqrt{-3})(p_2+\varepsilon_2q_2\sqrt{-3})\cdots(p_n+\varepsilon_nq_n\sqrt{-3})$$

其中 p_i,q_i 都是正整数，ε_i 等于 1 或 -1，并且 $p_i^2+3q_i^2$ 或者 4 或者是一个奇素数。

证明 设 $\alpha=a+b\sqrt{-3}$。如果 $N=a^2+3b^2$ 是偶数，则它可被 4 整除，如果 $N=a^2+3b^2$ 是不等于 1 的奇数，则它可被一个奇素数整除。因此如果 $N=a^2+3b^2$ 是不等于 1 的正整数，那么它的因数 P 就或者是 4，或者是一个奇素数。每当 $N=a^2+3b^2$ 分出一个因数时，由引理 9.5.7 和引理 9.5.8 可知 $\alpha=a+b\sqrt{-3}$ 就可相应地分出一个形如 $p+\varepsilon q\sqrt{-3}$ 的因数，其中 p,q 都是互素的有理整数。在此过程中，$\alpha=a+b\sqrt{-3}$ 每分出一个因数，它的模就严格减小，因此不断地从 $\alpha=a+b\sqrt{-3}$ 中分出因数，就可在有限步后，使得 $N\left(\dfrac{\alpha}{P_1P_2\cdots P_n}\right)=1$，这时

$$\frac{\alpha}{P_1P_2\cdots P_n}=u+v\sqrt{-3},\ u^2+3v^2=1$$

因而 $u=\pm1$，$v=0$，从而过程到此停止。因而 $\alpha=P_1P_2\cdots P_n$，其中每一个 P_i 都

具有形式 $P_i = p + \epsilon q\sqrt{-3}$，把所有 $p < 0$ 中的 -1 都提出来最后就得到

$$a + b\sqrt{-3} = \pm(p_1 + \epsilon_1 q_1\sqrt{-3})(p_2 + \epsilon_2 q_2\sqrt{-3})\cdots(p_n + \epsilon_n q_n\sqrt{-3})$$

其中 p_i, q_i 都是正整数，ϵ_i 等于 1 或 -1，并且 $p_i^2 + 3q_i^2$ 或者是 4 或者是一个奇素数。

引理 9.5.10 设 a, b 互素，那么在不计符号时 $a + b\sqrt{-3}$ 的因数是唯一确定的。

证明 由引理 9.5.9 知析出 $a + b\sqrt{-3}$ 的因数的过程就是从 $a^2 + 3b^2$ 析出因数 4 或奇因数 P 的过程。而由引理 9.5.7 和引理 9.5.8 可知如果在某一步析出因数 $p + q\sqrt{-3}$，则不可能析出因数 $p - q\sqrt{-3}$，并且反过来也是这样。因此如果 P 是 4，则显然从 $P = p^2 + 3q^2$ 除了符号外，就唯一地确定了。如果 P 是奇素数，并且 $a + b\sqrt{-3}$ 除了表示式

$$a + b\sqrt{-3} = (p + q\sqrt{-3})(u + v\sqrt{-3})$$

之外还有一个另外的表示式

$$a + b\sqrt{-3} = (p_1 + q_1\sqrt{-3})(u_1 + v_1\sqrt{-3})$$

那么由于

$$P^2 = P(u^2 + 3v^2) = P(u_1^2 + 3v_1^2)$$

我们就得出

$$N(u + v\sqrt{-3}) = N(u_1 + v_1\sqrt{-3})$$

这说明 $u + v\sqrt{-3}$ 和 $u_1 + v_1\sqrt{-3}$ 在 $Z[\sqrt{-3}]$ 中是相伴的，由此易证 $p + q\sqrt{-3}$ 和 $p_1 + q_1\sqrt{-3}$ 也是相伴的，而 $Z[\sqrt{-3}]$ 中的单位数只有 1 或 -1，因此 $p + q\sqrt{-3}$ 和 $p_1 + q_1\sqrt{-3}$ 至多相差一个符号。

由此就得出这一节的一个主要结果：

定理 9.5.1 设 a, b 是互素的，且 $a^2 + 3b^2$ 是一个立方数，则存在互素的有理整数 p, q 使得

$$a + b\sqrt{-3} = (p + q\sqrt{-3})^3$$

证明 由引理 9.5.9 的证明可设 $a^2 + 3b^2 = P_1P_2\cdots P_n$，其中 P_i 是 4 或者是一个奇素数。

如果因数中恰有 k 个 4，那么在 $a^2 + 3b^2$ 的素因子分解式中，2 的幂就是 2^{2k}，而由于 $a^2 + 3b^2$ 是一个立方数，所以就得出 $2k$ 必须是 3 的倍数，从而 k 必须是 3 的倍数。此外，任意奇素数的幂次也必须是 3 的倍数。即因数 $P_1, P_2, \cdots, P_n$ 的个数必须是 3 的倍数，且可以安排成每 3 个一组使得在同一组中的因数都是相同的。这也就是说可设

$$a^2 + 3b^2 = (P_1^2)(P_2^2)\cdots(P_n^2)$$

由于引理 9.5.10,在 $a+b\sqrt{-3}$ 的分解式中对应于 P_i 的因子 $p_i+q_i\sqrt{-3}$ 除符号外是唯一确定的,因此就得出

$$a+b\sqrt{-3}=(p_1+\varepsilon_1 q_1\sqrt{-3})^3(p_2+\varepsilon_2 q_2\sqrt{-3})^3\cdots(p_n+\varepsilon_n q_n\sqrt{-3})^3=(p+q\sqrt{-3})^3$$

由上式和 a,b 是互素的显然就得出 p,q 是互素的。由于

$$a^2+3b^2=\alpha\bar{\alpha}=(P_1P_2\cdots P_n)(\overline{P_1P_2\cdots P_n})$$

因此定理 9.5.1 是有理整数中命题。

设 $(a,b)=1,ab=c^k$,则 $a=u^k,b=v^k$,而且 $u=(a,c),v=(b,c)$(定理 3.4.6)的一种类似物,但是我们已经知道,$Z[\sqrt{-3}]$ 是一种性质和通常的整数很不相同的整环,例如在 $Z[\sqrt{-3}]$ 中并不成立素因数的唯一分解定理,一般来说不可约数和素数,既约和互素并不等价,甚至连最大公约数和最小公倍数都不存在。所以在 $Z[\sqrt{-3}]$ 中并没有一般的理论来导出一个上面定理的类似物。对具体的命题只能单独地给以具体证明,这就是我们上面讨论的内容,也正是这一形式上的类似显得有趣之处。

利用定理 9.5.1 就可解决 $n=3$ 时的费马问题,即

定理 9.5.2 设 $x>0,y>0,z>0,(x,y,z)=1$,则不定方程

$$x^3+y^3=z^3$$

不存在整数解。

为了证明这个定理,我们将证明一个比这个定理形式上更强的定理,即去掉 $x>0,y>0,z>0$ 的要求。也就是把 $x^3+y^3=z^3$ 的求解范围从原来的全体正整数扩大到全体整数。这样做的目的是为了使证明中所要讨论的情况少一些,从而使证明变得更紧凑。

首先,利用 $((x,y),z)=(x,(y,z))=(y,(x,z))=(x,y,z)=1$ 可以得出

$$(x,y)=(y,z)=(x,z)=1$$

因而 x,y,z 之中必有两个是奇数,一个是偶数。由于 $-x^3=(-x)^3$,因此在允许 x,y,z 可以取负值的情况下,我们可不妨假设 x,y 是奇数,z 是偶数。(这只要在方程中把偶数项移到方程右边,把奇数项移到左边即可)

由于费马问题是一个很有名的问题,近年来,它的最终解决又是一件很轰动的事,所以有不少介绍这一问题的科普读物和文章,但是不少这种书和文章中对上述假设的来源都没有交代清楚,上来就说不妨设 z 是偶数,这就使不少读者为此困惑不已。在此我可以十分肯定地说,如果没有允许 x,y,z 可以取负值的约定,而仅凭 $x^3+y^3=z^3$ 这一约束,是无法假设一定是偶数的。虽然我们无法直接举出反例(因为 $x^3+y^3=z^3$ 根本就没有整数解),但是我们可以间接地相信这一点。因为我们在作奇偶性讨论时,仅利用到奇数的乘方还是奇数,偶

数的乘方还是偶数，而根本没有用到乘方的具体次数，所以这种奇偶性讨论无论对多少次方都是成立的，而当 $n = 2$ 时，由著名的勾股数 $3^2 + 4^2 = 5^2$ 就可知道在逻辑上完全存在着 x 或 y 是偶数，而 z 是奇数的可能性。

定理 9.5.3 设 $xyz \neq 0, (x, y, z) = 1$，则不定方程

$$x^3 + y^3 = z^3$$

不存在整数解。

证明 利用 $((x, y), z) = (x, (y, z)) = (y, (x, z)) = (x, y, z) = 1$ 可以得出

$$(x, y) = (y, z) = (x, z) = 1$$

因而 x, y, z 之中必有两个是奇数，一个是偶数。由于 $-x^3 = (-x^3)$，因此在把方程中的偶数项移到方程右边，把奇数项移到左边即可后。我们可不妨假设 x，y 是奇数，z 是偶数。如果 $z < 0$，我们可在方程两边同乘以 -1 使 $z > 0$，因此我们可进一步设 z 是正偶数。于是 $\frac{x+y}{2}, \frac{x-y}{2}$ 都是整数，因而可设 $\frac{x+y}{2} = p$，$\frac{x-y}{2} = q$，于是有 $x = p + q, y = p - q$，其中 p, q 都是整数，并且从 x, y 互素和 $x = p + q, y = p - q$ 就得出 p, q 互素。

把 $x = p + q, y = p - q$ 代入方程就得到

$$x^3 + y^3 = 2p^3 + 6pq^2 = z^2$$

因而
$$\frac{p}{4}(p^2 + 3q^2) = \left(\frac{z}{2}\right)^3, pq \neq 0$$

由上式可以看出 p, z 的符号相同，因此 p 也是正整数。

由 x, y 是奇数和 $x = p + q, y = p - q$ 得出 p, q 之中一个是偶数，一个是奇数，因而 $p^2 + 3q^2$ 一定是奇数，由此得出一定有 $4 \mid p$。

以下分两种情况讨论：

(1) $3 \nmid z$。

由 $3 \nmid z$ 和 $\frac{p}{4}(p^2 + 3q^2) = \left(\frac{z}{2}\right)^3$ 首先得出 $3 \nmid p$。假设存在正的素数是 $\frac{p}{4}$ 和 $p^2 + 3q^2$ 的公因数，那么由 $3q^2 = p^2 + 3q^2 - 16\left(\frac{p}{4}\right)^2$ 就得出 $\pi \mid 3q^2$，因此 $\pi = 3$ 或 $\pi \mid q$。

但是由于 $3 \nmid p$，所以 $\pi \neq 3$。这样由 $\pi \mid \frac{p}{4}$ 因而 $\pi \mid p$ 和 $\pi \mid q$ 就得出 π 是 p, q 的公因数。由于 p, q 互素就得出 $\pi = 1$，因此 $\frac{p}{4}$ 和 $p^2 + 3q^2$ 互素。

由定理 3.4.6 和 $\frac{p}{4}(p^2 + 3q^2) = \left(\frac{z}{2}\right)^3$，$\frac{p}{4}$ 和 $p^2 + 3q^2$ 互素就得出

$$\frac{p}{4} = r^3, p^2 + 3q^2 = s^3$$

或 $$p = 4r^3, p^2 + 3q^2 = s^3$$

再由定理 9.5.1 就得出必存在互素的整数 u, v 使得

$$p = P_3(u, v) = u(u + 3v)(u - 3v)$$

$$q = Q_3(u, v) = 3v(u^2 - v^2)$$

因为 p 是偶数，而 p, q 是互素的，所以 q 是奇数，由此得出 v 是奇数，再由 u, v 互素就得出 u 是偶数。因此在 P_3 中 $u + 3v$ 和 $u - 3v$ 都是奇数。这样由 $4 \mid p$ 就得出 $4 \mid u$。

由于 $3 \nmid p$，故 $3 \nmid u$，由此得出 $(u, 3) = 1$，再由 $(u, v) = 1$ 得出

$$(u, -3v) = (u, u - 3v) = 1$$

以及 $$(u, 3v) = (u, u + 3v) = 1$$

又由 $u + 3v$ 是奇数得出 $(u + 3v, 2) = 1$，由 u, v 互素和 $(u, 3)$ 得出

$$(u + 3v, u) = (3v, u) = 1$$

得出 $$(u + 3v, u - 3v) = (u + 3v, 2u) = 1$$

因此 $u, u + 3v, u - 3v$ 是两两互素的。

于是由

$$\frac{p}{4} = \frac{u}{4}(u + 3v)(u - 3v) = r^3$$

就得出 $\frac{u}{4}, u + 3v, u - 3v$ 都是立方数，因而可设

$$\frac{u}{4} = a^3, u + 3v = b^3, u - 3v = c^3$$

从上式就得出

$$(-2a)^3 + b^3 + c^3 = 0$$

或 $$b^3 + c^3 = (2a)^3$$

不妨设 $a > 0$，于是

$$a^3 = \frac{u}{4} < r^3 = \frac{p}{4} < \left(\frac{z}{2}\right)^3$$

这就得出 $(2a)^3 < z^3$。因此我们从方程 $x^3 + y^3 = z^3$ 的一组解 (x, y, z)，$z > 0$ 又得出了一组解 $(b, c, 2a)$，$2a > 0$，而 $2a < z$。于是根据欧拉的无穷递降法就得出在情况(1)下，不定方程 $x^3 + y^3 = z^3$，$xyz \neq 0$，$(x, y, z) = 1$ 不存在整数解。

(2) $3 \mid z$。

由 $3 \mid z$ 得出 $3 \mid p$，而由 p, q 互素又得出 $3 \nmid q$。因此由 $\frac{p}{4}(p^2 + 3q^2) = \left(\frac{z}{2}\right)^3$ 就得出

$$\frac{p}{36}\left(q^2 + 3\left(\frac{p}{3}\right)^2\right) = \left(\frac{z}{6}\right)^3$$

设 π 是$\frac{p}{36}$和 $q^2+3\left(\frac{p}{3}\right)^2$ 的公因数，则 $\pi \mid q^2+3\left(\frac{p}{3}\right)^2-12\cdot\frac{p}{36}=q^2$，因而 $\pi \mid q$，再由 $\pi \mid \frac{p}{36}$ 得出 $\pi \mid p$，因此 $\pi \mid (p,q)=1$。这就得出 $\pi=1$，因此$\frac{p}{36}$和$q^2+3\left(\frac{p}{3}\right)^2$ 互素。

由定理3.4.6和$\frac{p}{36}\left(q^2+3\left(\frac{p}{3}\right)^2\right)=\left(\frac{z}{6}\right)^3$，$\frac{p}{36}$和 $q^2+3\left(\frac{p}{3}\right)^2$ 互素就得出$\frac{p}{36}$和 $q^2+3\left(\frac{p}{3}\right)^2$ 都是立方数。再由定理9.5.1得出必存在互素的 u,v 使得

$$p=36r^3,q=P_3(u,v)=u(u+3v)(u-3v),\frac{p}{3}=3v(u+v)(u-v)$$

由于 q 是奇数，故从上式得出 u 是偶数，再从 u,v 互素又得出v 是奇数，此外，由上面的式子还得出

$$-8r^3=2v(v+u)(v-u)$$

设 π 是$2v,v+u,v-u$ 的公因数，则由 $\pi \mid v+u$，$v+u$ 是奇数得出$(\pi,2)=1$，因此 $\pi \mid y$，故 $\pi \mid (y,y+u)=(v,u)=1$，$\pi=1$，由此得出 $2v,v+u,v-u$ 是两两互素的。于是由 $-8r^3=2v(v+u)(v-u)$ 就得出 $2v,v+u,v-u$ 都是立方数，因而可设

$$2v=a^3,v+u=b^3,v-u=c^3$$

$$b^3+c^3=a^3$$

不妨设 $a>0$，于是 $a^3=2v<8r^3<9r^3=\frac{p}{4}\left(\frac{z}{2}\right)^3<z^3$。因此我们从方程 $x^3+y^3=z^3$ 的一组解(x,y,z)，$z>0$又得出了一组解(b,c,a)，$a>0$，而 $a<z$。于是再次根据欧拉的无穷递降法就得出在情况(2)下，不定方程 $x^3+y^3=z^3$，$xyz\neq 0$，$(x,y,z)=1$ 不存在整数解。

综合上述两种情况就证明了定理。

我们上面的证明几乎是逐字逐句按照欧拉的原著而做出的，但是欧拉虽然天才地给出了这一证明的思想，却并没有证明定理9.5.1，他认为这是当然成立的，幸运的是，尽管在手续上不够严格，但是不管怎么说，结论却是对的，所以幸运之星再一次照耀到了欧拉头上(我们说再一次是由于欧拉不只一次地使用现在看来不严格的手段去得出一些结果，例如在级数求和中，但是他不只一次幸运地得出了正确的结果，所以欧拉的运气真是好，幸运之星不只一次地眷顾过他)。

我认为即使欧拉在得出定理9.5.3时有不够严格之处，我们仍能从欧拉那里学到许多有益的东西。那就是在我们思考问题时，可以先不管严格性，而让我们的思想大胆地飞驰，以致能够看出一些问题的本质乃至猜出结论，然后再研究严格性，看看这些结论是否能严格地证明出来。说老实话，严格性只是一种技

术手段，但是最宝贵的是解题的思想。当然在你把东西写出来时，这二者缺一不可。

习题9.5

1. 设 a,b 互素，证明：形如 a^2-2b^2 的整数的任一因数仍具有 a^2-2b^2 的形式。

2. 设 $p=8n+3$ 是素数，$x=\frac{p+1}{2}$。证明：

(1) $p \mid x^{8n+2}-1$；

(2) $p \mid x^{8n}(p+1)^2-4$；

(3) $p \mid (x^{4n}-2)(x^{4n}+2)$；

(4) 利用第1题证明 $p \nmid x^{4n}-2$，因此 $p \mid x^{4n}+2$；

(5) 证明：p 必可表示成 a^2+2b^2 的形式。

3. 从 $1^{8n},2^{8n},\cdots,m^{8m},\cdots$ 开始做各级差分，证明：

(1) 上述差分表的第一行的每一项都具有形式 $a^{8n}-b^{8n}=(a^{4n}-b^{4n})(a^{4n}+b^{4n})$；

(2) $a^{4n}+b^{4n}$ 可以写成 a^2+2b^2 的形式；

(3) 每个形如 $8n+1$ 的素数 p 都可写成 a^2+2b^2 的形式。

4. 设 a,b 互素，a^2+2b^2 是一个立方数，证明：必存在互素的整数 p,q 使得

$$a+b\sqrt{-2}=(p+q\sqrt{-2})^3$$

5. 设 a,b 互素，a^2+b^2 是一个立方数，证明：必存在互素的整数 p,q 使得

$$a+b\sqrt{-1}=(p+q\sqrt{-1})^3$$

6. 证明：不定方程 $x^2+4=y^3$，x 是奇数的唯一解是 $11^2+4=5^3$。

7. 证明：

(1) 如果 $x^2+4=y^3$，x 是偶数，则 $x=\pm 2$，因而 $2 \mid y$；

(2) 令 $u=\frac{x}{2}$，$v=\frac{y}{2}$，将上述方程化为 $u^2+1=2v^3$；

(3) 证明：$v^3=\frac{u^2+1}{2}$ 是一个形如 a^2+b^2 的平方和，其中 $a-b=1$，因而 a,b 互素；$(u^2+1=(u+\mathrm{i})(u-\mathrm{i}),2=(1+\mathrm{i})(1-\mathrm{i}))$

(4) 利用5证明：$1=(p+q)(p^2-4pq+q^2)$，$u=(p-q)(p^2+4pq+q^2)$；

(5) 利用(4)得出 $p+q=p^2-4pq+q^2=\pm 1$，因而 $pq=0$，从而 $x=\pm 2$；

(6) 证明：不定方程 $x^2+4=y^3$ 的唯一解是 $11^2+4=5^3$ 和 $2^2+4=2^3$。

8. (1) 设 a,b 是不同时等于1的互素的正整数，证明：$1+ab$ 不可能整除 a^2+b^2；

(2) 证明:如果正整数 a,b 使得 $1+ab\mid a^2+b^2$,则$\frac{a^2+b^2}{1+ab}$必是一个完全平方数;

(3) 举出 $a>1,b>1$,且 $1+ab\mid a^2+b^2$ 的实际例子。

9.6 复数的推广

哈米尔顿(Hamilton, William Rowan, 1805—1865),英国数学家,物理学家,生于爱尔兰的都柏林,卒于都柏林附近的邓辛克天文台.

由于复数的建立获得了巨大的成功,因此在复数出现后,有人就在考虑是否能把复数推广到空间中去的问题,也就是考虑是否能建立一种与复数类似的三元数的问题。其中爱尔兰数学家哈米尔顿爵士对此问题作了长期的思考。从19世纪20年代后期开始,哈米尔顿便开始了对复数进行从二维到三维的扩展的研究。在19世纪30年代,哈米尔顿构想了多种三元数的方案,但都以失败而告终。1843年,他再次挑战这一问题,并再次遭遇失败,但这一次,他没有空手而归,在失败后,他放弃了构造三元数的企图,并转而完成了四元数的构造。据他自己在日记中记载1843年10月16日,他和妻子沿着皇家运河散步,突然一个念头像闪电般出现,即,这么样处理四元数中 i,j,k 三者的乘积,他是那么的兴奋,于是用小刀在布尔罕桥上的石头刻上最初出现的公式。他自己把这一结果看成是他一生中最伟大的数学成就,并为此倾注了他后半生的全部时间和精力。

哈米尔顿是一个很有才能的人,但为什么哈米尔顿一直无法完成对三元数的构建呢?现在看来,答案是很简单的,那就是由于这是一件不可能完成的事。由于很多科普方面的书籍都讲到过哈米尔顿和四元数的故事,所以许多读者对此并不陌生。但对于为什么不可能构建三元数,有些读者可能就不知道了,好像讲到这些内容的书也不太多。

要了解为什么不可能构建三元数,我们必须了解从已有的数系上再去构建一种新的数系需要遵守什么原则。根据我们以往多次扩充数系的做法,可以总结出以下几条数系扩充原则:

(1) 集合继承性。即作为集合,一般应有:原有的数系属于新的数系。

(2) 性质继承性。即要求新的数系及其中的运算尽可能地具有原有数系的性质。

(3) 封闭性。即在一种数系中,数系中的数经过运算后仍然要属于这一数系。

(4) 新数与原有数的无关性。即新数不可能表示成原有数的线性组合(组合的系数是原有的数)。

继承性的要求的意义在于使得我们可以以最小的代价来获得新的工具。从整数开始，我们已对数进行了多次扩充如下

正整数 → 整数 → 有理数 → 实数 → 复数

设想如果没有继承性，那么每一次扩充后，我们将面临一种完全新的，我们所不熟悉的对象。那对我们将是一种多么大的负担啊。你只要想一下，仅仅一个正整数加正分数就用掉了小学6年的时间，又用了初中3年的时间去学习有理数和实数(老实说，初中学的那点关于实数的知识，只不过让你沾了点边，要真正了解实数，还要到大学)，又用了高中3年的时间去学习复数。这还是在有继承性的情况下如此，如果没有继承性，我们的学习负担那就简直不可想象了。

至于封闭性的要求显然也是不可少的。如果没有这一条，那只能说明你建立的这个数系是不完善的。

无关性的要求也是不可少的。如果"新"的数可以表示成原有的数的线性组合(组合系数是原有的数)，那么根据原有的数系的封闭性就可知道，你所定义的所谓"新"的数根本不新，它本来就是一种已知的对象。既然如此，也就没有扩充的必要了。

现在再来看，当初i这个东西，我们是为了使方程 $x^2=-1$ 有解而引入的，因此i天然的就具有性质 $i^2=-1$。下面我们要证明，按照继承性的要求，在二元数中，作为一种新的符号，i必然具有性质 $i^2=-1$。

定义 9.6.1 称 $\alpha=a+bi$ 是二元数，其中 a,b 都是实数，i是一个新的与实数无关的数。类似的，称 $\alpha=a+bi+cj$ 是三元数，其中 a,b,c 都是实数，i，j是新的与实数无关的数，同时i与j也是无关的；称 $\alpha=a+bi+cj+dk$ 是四元数，其中 a,b,c,d 都是实数，i，j，k是新的与实数无关的数，同时i，j，k本身也是两两无关的。

根据继承性的要求，当我们构建二元数时，有三方面的来源可供继承：

(1) 运算方面的来源。即可以定义两种运算：加法和乘法，并且这两种运算满足加法交换律、加法结合律、乘法交换律、乘法结合律以及乘法对于加法的分配律。

(2) 顺序方面的来源。即实数顺序性的不等式性质。

(3) 几何方面的来源。即对每个数 α 可定义一种被称为模的非负数 $N(\alpha)$，使得当把 α 看成向量时，$N(\alpha)$ 就是此向量的长度。并且 $N(\alpha)$ 具有性质 $N(\alpha\beta)=N(\alpha)N(\beta)$。

引理 9.6.1 如果在二元数中，符号i具有性质：$i^2=-\lambda$，其中 λ 是一个正实数，则这种二元数不可能与实数的顺序性质相容。

证明 我们证在i和0之间就不可能建立实数中的顺序关系。

由无关性，i不可能等于0，因此只可能 $i>0$ 或 $i<0$。

如果 $i>0$,那么由实数的顺序性,应有 $i^2>0$,但是又有 $i^2=-\lambda<0$,矛盾。

如果 $i<0$,那么 $-i>0$,因此 $-i^2<0$,但是又有 $-i^2=\lambda>0$,矛盾。

这就说明,在这种二元数中,无法建立实数的顺序性质。

引理 9.6.2 仅由继承性的运算来源,不可能唯一地确定二元数。

证明 设 λ 是一个正实数。那么由规定 $i^2=-\lambda$ 以及实数的运算性质就可以确定二元数的运算。设 $\alpha=a+bi$,再规定 $N(\alpha)=a^2+\lambda b^2$,那么可以验证 $N(\alpha)$ 具有性质 $N(\alpha\beta)=N(\alpha)N(\beta)$。

由于对每一个 λ 就确定了一种二元数,所以由继承性的运算来源可以确定无穷多种二元数,这就证明了引理。

当然,通过引入同构概念,你可以认为这无穷多种二元数的本质是一种,但是我们不准备如此讨论下去,至少从形式上看,仅由继承性的运算来源,不可能唯一地确定二元数。

引理 9.6.3 由继承性的运算来源和几何来源唯一地确定了二元数,在这种二元数中,符号 i 必然具有性质 $i^2=-1$。

证明 首先由继承性的几何来源,对二元数 $\alpha=a+bi$,$N(\alpha)$ 必须具有形式

$$N(\alpha)=\sqrt{a^2+b^2}$$

由此得出 $N(1)=N(i)=1$。再由模的性质

$$N(\alpha\beta)=N(\alpha)N(\beta)$$

得出

$$N(i^2)=N(i^3)=1$$

由封闭性,i^2 仍是一个二元数,因此可设 $i^2=a+bi$,这样

$$i^3=i\cdot i^2=i(a+bi)=ai+bi^2=ai+b(a+bi)=ab+(a+b^2)^2i$$

由 $N(i^2)=N(i^3)=1$ 得出

$$a^2+b^2=1$$

$$a^2b^2+(a+b^2)^2=1$$

由此得出 $a^2b^2+(a+b^2)^2-a^2-b^2=(a^2+2a-1+b^2)b^2=0$

因此 $b=0$ 或 $a^2+2a-1+b^2=0$。

如果 $a^2+2a-1+b^2=0$,那么 $1=a^2+b^2=1-2a$,因此 $a=0,b=\pm1$,因而 $i^2=\pm i$。由无关性 $i\neq0$,因此 $i=\pm1$。而这又与无关性矛盾。这就说明不可能有 $a^2+2a-1+b^2=0$。因而只能有 $b=0,a=\pm1$。但是如果 $a=1$,那我们就得出 $i^2=1$,因此 $i=\pm1$。再次与无关性矛盾。所以我们最后只能有 $a=-1$,即 $i^2=-1$。

由引理9.6.1～引理9.6.3可知,在二元数中,继承性的三个来源不可能相容,所以要建立二元数就必须放弃其中某个来源。一般我们认为放弃运算来源和几何来源代价太大,因此我们只能放弃实数的顺序性质,这就是目前的复数。

因此如果承认继承性的运算来源和几何来源，我们就只能得出唯一的一种二元数，就是复数。

上面我们已经看到，当把通常的实数扩充到二元数时，我们必须牺牲顺序性，下面我们可以看到，当我们企图进一步扩充数系时，我们还要牺牲掉实数的更多特性。

首先是乘法的交换性在三元以上的数系中不可能成立。

引理 9.6.4 如果承认继承性的运算来源和几何来源，那么在三元以上的数系中不可能成立乘法交换律。

证明 由于三元数是元数的子集（只要在 n 元数集合中，从第四个元之后的系数一律取 0 即可得到三元数集合），故只要对三元数证明即可。

在三元数中有两个二元数集合：$\{a+bi\}$ 和 $\{a+bj\}$，它们作为二元数系是封闭的，因此由引理 9.6.3 我们得出在三元以上的数系中必有 $i^2=j^2=k^2=-1$。

假设在这些数系中成立乘法交换律，那么就有

$$(i+j)(i-j)=i^2-j^2=0$$

因此 $i+j=0$ 或 $i-j=0$，但是无论发生哪种情况，这都与无关性矛盾。

此外，我们还可以证明在三元数系中，实数的模的性质不可能再保留。

引理 9.6.5 在三元数系中不可能继承模的几何意义和乘法性质，即设 $\alpha=a+bi+di$，则不可能定义一个模 $N(\alpha)$ 使得 $N(\alpha)=\sqrt{a^2+b^2+c^2}$，并且 $N(\alpha\beta)=N(\alpha)N(\beta)$。

证明 设 $\alpha=1+i+j$，$\beta=1+2i+4j$，由于 α 和 β 都是三元整数，所以 $\alpha\beta$ 也应是 3 元整数（就像在复整数中那样）。因此可设 $\alpha\beta=a+bi+cj$，其中 a，b，c 都是有理整数。则 $N(\alpha)=\sqrt{3}$，$N(\beta)=21$。如果 $N(\alpha\beta)=N(\alpha)N(\beta)$ 成立，那么就应有

$$\sqrt{a^2+b^2+c^2}=\sqrt{3}\cdot\sqrt{21}=\sqrt{63}$$

因而应有

$$a^2+b^2+c^2=63$$

但是易于证明，对任意整数 a,b,c，$a^2+b^2+c^2\not\equiv-1 \pmod 8$，$63\equiv-1 \pmod 8$，因此

$$a^2+b^2+c^2\neq 63$$

这一矛盾就说明了在三元数系中不可能定义一个模 $N(\alpha)$ 使得 $N(\alpha)=\sqrt{a^2+b^2+c^2}$，并且 $N(\alpha\beta)=N(\alpha)N(\beta)$。

由引理 9.6.4 和引理 9.6.5 就得出

引理 9.6.6 不可能建立与继承性的运算来源和几何来源相容的三元数系。

引理 9.6.7 不可能有封闭的三元数系。

证明 假设三元数系可以封闭,那么由封闭性,ij 也是一个三元数,于是可设

$$ij = a + bi + cj$$

其中 a,b,c 都是实数,于是

$$1 = i^2j^2 = i(ij)j = i(a + bi + cj)j = aij - bj - ci = \\ a(a + bi + cj) - bj - ci = \\ a^2 + (ab - c)i + (ac - b)j$$

在上式中比较等式两边的同类项就得到 $a = 1, b = c$ 或 $a = -1, b = -c$。因此 $ij = 1 + bi + bj$ 或者 $ij = -1 + bi - bj$。

如果 $ij = 1 + bi + bj$,则在等式两边乘以 i 后得到

$$-j = i - b + bij = i - b + b(1 + bi + bj) = i + b^2i + b^2j$$

因此得出 $b^2 = -1$,矛盾。

如果 $ij = -1 + bi - bj$,则在等式两边乘以 i 后得到

$$-j = -i - b - bij = -i - b - b(-1 + bi - bj) = -i - b^2i + b^2j$$

仍得出 $b^2 = -1$,矛盾。

在经过长时期的思考后,哈米尔顿也认识到必须放弃乘法交换律,并且三个元不够(因为 ij 要"出去")。这以后,他又长时间地为如何定义四元数的乘法而苦恼。直到终于有一天在桥上得到了顿悟。我们已无法得知他是如何顿悟的,但是从他把四元数的乘法公式刻在桥上可以想象这一公式不会太长。

我们只能猜测一种可能的顿悟方式是既然 ij 要"出去",于是可设 $ij = k$,其中 k 是一个新的元,然而由对称性,jk,ki 也要"出去",但是我们现在已经有四个元了,因此 jk,ki 的"出去"不能像 ij 那样靠设新的元的办法,因而只能"回来",而既然 $ij = k$ 恰是另一个元,那么根据对称性,jk,ki 也应该有形同的形式。这样一种合乎逻辑的办法是让 $ij = k, jk = i, ki = j$,一旦悟到这一点,可以说建立四元数的工作就基本完成了。剩下的事就是证明下面的乘法反交换律。

引理 9.6.8 在四元数的基元 i,j,k 之间成立乘法反交换律,即

$$ij = -ji, ik = -ki, jk = -kj$$

证明 由于 i,j,k 是基元,故由引理 9.6.3 知必有 $i^2 = j^2 = k^2 = -1$。因此有

$$(ij)(ji) = i(j^2)i = -i^2 = 1 = -k^2 = -(ij)(ij)$$

由于 $ij \neq 0$(否则得出 $i = 0$ 或 $j = 0$,与无关性矛盾),因而从上式就得出 $ji = -ij$。同理可证其余几式。

可以验证,在规定

(1) $i^2 = j^2 = k^2 = -1$;

(2) $ij = k, jk = i, ki = j$;

(3) $ij = -ji, ik = -ki, jk = -kj$。

下，就可按照多项式乘法的法则顺利地定义四元数的乘法，因而这个困扰哈密尔顿多年来的难题就获得了解决。

由直接计算可证下面的

定理 9.6.1

(1) 在规定

(i) $i^2 = j^2 = k^2 = -1$;

(ii) $ij = k, jk = i, ki = j$;

(iii) $ij = -ji, ik = -ki, jk = -kj$。

下，四元数集合构成一个有单位元的不可交换的体或除环，称为四元数体(除环)或哈米尔顿体或哈米尔顿除环。其中的加法和乘法满足加法交换律、加法结合律、乘法结合律以及乘法关于加法的分配律。

(2) 设 $\alpha = a + bi + cj + dk$，定义 α 的共轭 $\bar{\alpha}$，迹 $T(\alpha)$ 和 $N(\alpha)$ 模为

$$\bar{\alpha} = a - bi - cj - dk$$

$$T(\alpha) = \alpha + \bar{\alpha} = 2a, N(\alpha) = \sqrt{\alpha\bar{\alpha}} = \sqrt{a^2 + b^2 + c^2 + d^2}$$

则

$$N(\alpha\beta) = N(\alpha)N(\beta)$$

定义 9.6.2 设 V 是一个非空集合，P 是一个域，在集合 V 的元素之间定义了一种称为加法的运算，在 P 与集合 V 的元素之间定义了一种称为数量乘法的运算，如果这两种运算满足以下法则，则称 V 是 P 上的线性空间。

(1) 加法构成一个加群，即加法满足加法交换律和结合律，存在加法单位元(0 元素)以及加法的逆元(负元素)。

(2) 数量乘法满足

(i) $1 \cdot \alpha = \alpha, 1 \in P, \alpha \in V$;

(ii) $k(h\alpha) = (kh)\alpha, k, h \in P, \alpha \in V$;

(iii) 数量乘法满足对于加法的分配律，即

$$(k + h)\alpha = k\alpha + h\alpha, k, h \in P, \alpha \in V$$

$$k(\alpha + \beta) = k\alpha + k\beta, k \in P, \alpha, \beta \in V$$

容易证明，线性空间具有以下性质：

引理 9.6.9 设 V 是 P 上的线性空间，则 V 有以下性质：

(1) 0 元素是唯一的；

(2) 负元素是唯一的；

(3) $0 \cdot \alpha = 0; k \cdot 0 = 0; (-1) \cdot \alpha = -\alpha$;

(4) 如果 $k \cdot \alpha = 0$，那么 $k = 0$ 或 $\alpha = 0$。

在线性空间的元素之间可以定义所谓线性相关的概念。

定义 9.6.3 线性空间 V 中的元素 $\alpha_1,\alpha_2,\cdots,\alpha_r(r\geqslant 1)$ 称为线性相关，如果 P 中存在 r 个不全为 0 的数 $k_1,k_2,\cdots,k_r$ 使得

$$k_1\alpha_1+k_2\alpha_2+\cdots+k_r\alpha_r=0$$

如果 $\alpha_1,\alpha_2,\cdots,\alpha_r$ 不是线性相关的，则称它们是线性无关的。也就是说 $\alpha_1,\alpha_2,\cdots,\alpha_r$ 线性无关的充分必要条件是从等式 $k_1\alpha_1+k_2\alpha_2+\cdots+k_r\alpha_r=0$ 可以得出

$$k_1=k_2=\cdots=k_r=0$$

定义 9.6.4 设 V 是 P 上的线性空间，则称 V 中线性无关元素的最大个数为 V 的维数。

定义 9.6.5 设 V 是 P 上的线性空间，如果 V 的维数是有限的，则称 V 是有限维空间，否则称 V 是无限维空间。

定义 9.6.6 设 P 上的线性空间 V 是 n 维的，那么 V 中任意 n 个线性无关的元素 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 称为 V 的一组基。

定理 9.6.2 设 P 上的线性空间 V 是 n 维的，$\alpha_1,\alpha_2,\cdots,\alpha_n$ 是 V 的一组基，那么 V 中任意一个元素 α 可被 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 线性表出，即

$$\alpha=k_1\alpha_1+k_2\alpha_2+\cdots+k_n\alpha_n,k_1,k_2,\cdots,k_n\in P$$

其中系数 $k_1,k_2,\cdots,k_n$ 由 α 和基 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 唯一确定。

证明 由于 V 是 n 维的，根据维数的定义就知道 V 中线性无关元素的最大个数为 n。于是 $n+1$ 个元素 α 和 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 必然线性相关，因此 α 可被 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 线性表出，即存在 $k_1,k_2,\cdots,k_n\in P$ 使得 $\alpha=k_1\alpha_1+k_2\alpha_2+\cdots+k_n\alpha_n$。

假如 α 还有另一种表示方法为

$$\alpha=k'_1\alpha_1+k'_2\alpha_2+\cdots+k'_n\alpha_n$$

那么由

$$(k'_1-k_1)\alpha_1+(k'_2-k_2)\alpha_2+\cdots+(k'_n-k_n)\alpha_n=0$$

和 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 的形性无关性即可知道必有 $k'_1=k_1,k'_2=k_2,\cdots,k'_n=k_n$，因此上述表法是唯一的。

定义 9.6.7 如果环 M 同时是 P 上的有限维线性空间，并且满足条件

$$(k\alpha)\beta=\alpha(k\beta)=k(\alpha\beta),k\in P,\alpha,\beta\in M$$

那么就称 M 是 P 上的一个超复系或结合代数。

如果 M 是除环，则称此代数是可除代数。

由上述定义可知，代数与环的区别在于，一个代数不仅是环，而且还具有线性空间的结构，而由于线性空间有基。这就使得代数中的结构比环要更清楚，具体说来，你只要搞清了代数中基元素的性质，那么代数中任意元素的性质就确定了。

前面我们从继承性的几条要求确定了二元数只能是复数，同时得到了一个

复数的推广——四元数。这样，我们就得到了实数、复数和四元数共三个有限维可除代数的例子。这自然引出一个问题，即是否还有其他的例子？不过，由于我们用到了模这个概念，而这个概念是来自几何方面的，从代数本身并没有引入这一概念的必然性。因此我们还想知道，在研究是否还有其他的有限维可除代数这个问题上，是不是能避开模这个概念。下面我们就来回答这些问题。

引理 9.6.10 一维的可除代数 K 同构于实数体 R。

证明 设 e 是 K 中的单位元，$\alpha \in R$ 是任意实数，那么映射 $\sigma(\alpha) = \alpha e$ 显然是 1—1 的，并且是 K 和 R 之间的同构，这就证明了引理。

引理 9.6.11 作为二维可除代数的二元数体 K 同构于复数体 C。

证明 由于 K 是一元数的扩展，因此 K 中必有一个子空间是一维的可除代数。由引理9.6.10知，此子空间同构于实数体 R，于是我们不妨设这个子空间就是 R。

由于 K 是二元数，所以 K 中必含有一个不是实数的元素 α，根据无关性的要求，$1,\alpha$ 是线性无关的，因此它们构成 K 的一组基。再根据封闭性可知 $\alpha^2 \in K$，因此 α^2 必可被 $1,\alpha$ 线性表出，故可设 $\alpha^2 = p + q\alpha, p, q \in R$。因此 α 满足方程

$$\alpha^2 - q\alpha - p = 0$$

这个二次方程的判别式为 $\Delta = q^2 + 4p$。由于 α 不是实数，因此必有 $\Delta < 0$。设

$$\mathrm{i} = \frac{2\alpha - q}{\sqrt{-\Delta}}$$

则

$$\mathrm{i}^2 = -\frac{1}{\Delta}(2\alpha - q)^2 = -\frac{1}{\Delta}(4\alpha^2 - 4q\alpha + q^2) = -\frac{1}{\Delta}(4p + q^2) = -\frac{1}{\Delta}\cdot\Delta = -1$$

显然 $1,\mathrm{i}$ 是线性无关的（否则 $1,\alpha$ 将是线性相关的）。于是 $1,\mathrm{i}$ 构成 K 的一组基，而 K 中任意元素可表示成 $a + b\mathrm{i}, a, b \in R, \mathrm{i}^2 = -1$ 的形式，这就表明 K 就是复数体 C。

引理 9.6.12 作为四维可除代数的四元数体 K 同构于四元数体 H。

证明 由 K 是四维的可知 K 中存在三个线性无关的元素 $1,\mathrm{i},u$。并且由引理 9.6.11 的证明可知由 $1,\mathrm{i}$ 生成的子空间同构于复数体，因而有 $\mathrm{i}^2 = -1$，同理有 $u^2 = -1$。

由于 $1,\mathrm{i},u$ 是线性无关的，所以 $1,\mathrm{i}+u$ 也是线性无关的，因而把 $\mathrm{i}+u$ 像 i 或 u 那样看成引理9.6.11中的 α，由与前面同样的道理知可设 $(\mathrm{i}+u)^2 = a(\mathrm{i}+u) + b$，同理，可设 $(\mathrm{i}-u)^2 = c(\mathrm{i}-u) + d$。于是把这两个式子相加就得到

$$-4 = b + d + (a + c)\mathrm{i} + (a - c)u$$

由于 $1,\mathrm{i},u$ 线性无关，因此 1，就得到 $a + c = 0, a - c = 0$，故 $a = c = 0$。由此得出

$$iu + ui = b + 2 = 2t, t \in R$$

令 $v = u + ti$，则

$$iv + vi = i(u + ti) + (u + ti)i = iu + ui - 2t = 0$$

同时又有

$$v^2 = (u + ti)^2 = u^2 + uti + tui - t^2 =$$
$$-1 + t(ui + iu) - t^2 = -1 + 2t^2 - t^2 = t^2 - 1$$

由于 v 显然不是实数，因此必有 $t^2 - 1 < 0$，于是可记 $v^2 = -s^2$，因而如果记 $j = \frac{v}{s}$，则 $j^2 = -1$，并且

$$ij + ji = \frac{iv + vi}{s} = 0$$

这就得出 $ij = -ji$。

再令 $ij = k$，那么

$$k^2 = ijij = ij(-ji) = -ij^2i = i^2 = -1$$
$$ki = iji = -iij = -ik = j$$

同理可得 $jk = -kj = i$。

由于 $1, i, u$ 是线性无关的，因而易证 $1, i, u + ti, ui - t$ 无关，由此又得出 $1, i, u + ti, i(u + ti)$ 无关，因而 $1, i, v, iv$ 无关，由此再得出 $1, i, j, ij$ 无关，这也就是 $1, i, j, k$ 是线性无关的。这就证明了 K 就是四元数体 H。

引理 9.6.13 不可能存在作为可除代数的元数大于 4 的多元数体 K。

证明 假设存在这样的数体 K，则由引理 9.6.13 的证明可知，K 中将存在 5 个线性无关的元素 $1, i, j, k, h$ 使得 $h^2 = -1$，并且

$$ih + hi = a, jh + hj = b, kh + hk = c, a, b, c \in \mathbf{R}$$

但是我们又有

$$hk = (hi)j = (a - ih)j = aj - ihj = aj - i(b - jh) =$$
$$aj - bi + ijh = aj - bi + kh = aj - bi + c - hk$$

因而有

$$2hk = aj - bi + c$$

在上式两边右乘 k 就得出

$$ai + bj + ck = -2h$$

上式与 $1, i, j, k, h$ 是线性无关的矛盾。所得的矛盾就证明了不可能存在引理中所说的多元数体。

由引理 9.6.10、引理 9.6.11、引理 9.6.12、引理 9.6.17 和引理 9.6.13 就得出

定理 9.6.3(弗罗贝尼乌斯定理) 除了实数域、复数域和四元数体三种代数外，不可能存在其他与此不同构的实数域上的有限维可除代数。

费罗贝尼乌斯（Frobenius，Fer dinand Georg，1849—1917），德国数学家。生于柏林，卒于柏林夏洛滕堡。

习题 9.6

1. 计算

(1) $(-1+2\mathrm{i}-3\mathrm{j}+k)(2-\mathrm{i}+3\mathrm{j}-2\mathrm{k})$

(2) $(a_1\mathrm{i}+a_2\mathrm{j}+a_3\mathrm{k})(b_1\mathrm{i}+b_2\mathrm{j}+b_3\mathrm{k})$

2. 设 α,β 表示四元数,证明:

(1) $\overline{\alpha+\beta}=\overline{\alpha}+\overline{\beta}$;

(2) $\overline{\alpha\beta}=\overline{\beta}\,\overline{\alpha}$;

(3) $N(\alpha\beta)=N(\alpha)N(\beta)$;

(4) 证明:当 $\gamma\neq 0$ 时,$T(\gamma^{-1}\alpha\gamma)=T(\alpha)$,$N(\gamma^{-1}\alpha\gamma)=N(\alpha)$;

(5) α 适合二次方程 $x^2-T(\alpha)x+N^2(\alpha)=0$。

3. 设 α,β 表示四元数,$\alpha\neq 0$,证明:

(1) α 存在唯一的倒数 α^{-1};

(2) $(\alpha\beta)^{-1}=\beta^{-1}\alpha^{-1}$。

4. 设 $\alpha=a+b\mathrm{i}+c\mathrm{j}+d\mathrm{k}$,$z_1=a+b\mathrm{i}$,$z_2=c+d\mathrm{i}$,证明:

(1) $\alpha=z_1+z_2\mathrm{j}$;

(2) $N(\alpha)=\sqrt{N^2(z_1)+N^2(z_2)}$,$\overline{\alpha}=\overline{z}_1-z_2\mathrm{j}$;

(3) $\alpha^{-1}=\dfrac{\overline{z_1}-z_2\mathrm{j}}{N^2(\alpha)}$

5. 决定四元数体的中心。

6. 证明:

$$(a_1^2+a_2^2+a_3^2+a_4^2+a_5^2+a_6^2+a_7^2+a_8^2)(b_1^2+b_2^2+b_3^2+b_4^2+b_5^2+b_6^2+b_7^2+b_8^2)=$$
$$(a_1b_1+a_2b_2+a_3b_3+a_4b_4+a_5b_5+a_6b_6+a_7b_7+a_8b_8)^2+$$
$$(a_1b_2-a_2b_1-a_3b_4+a_4b_3-a_5b_6+a_6b_5-a_7b_8+a_8b_7)^2+$$
$$(a_1b_3+a_2b_4-a_3b_1-a_4b_2+a_5b_7-a_6b_8-a_7b_5+a_8b_6)^2+$$
$$(a_1b_4-a_2b_3+a_3b_2-a_4b_1-a_5b_8-a_6b_7+a_7b_6+a_8b_5)^2+$$
$$(a_1b_5+a_2b_6-a_3b_7+a_4b_8-a_5b_1-a_6b_2+a_7b_3-a_8b_4)^2+$$
$$(a_1b_6-a_2b_5+a_3b_8+a_4b_7+a_5b_2-a_6b_1-a_7b_4-a_8b_3)^2+$$
$$(a_1b_7+a_2b_8+a_3b_5-a_4b_6-a_5b_3+a_6b_4-a_7b_1-a_8b_2)^2+$$
$$(a_1b_8-a_2b_7-a_3b_6-a_4b_5+a_5b_4+a_6b_3+a_7b_2-a_8b_1)^2$$

7. 仿照引理 9.6.11 和引理 9.6.12 证明:有限维可除代数中的任意元素 α 都可表为 1 和 α 的线性组合。

第十章 多项式

10.1 多项式及其基本性质

我们从中学起就已很熟系什么是多项式了，并且也知道如何对多项式进行加、减、乘、除等四则运算。不过为了明确和统一符号起见，我们仍对某些重要概念和法则重新定义和提到，你如果已经很熟系这些内容，可以把它看成是一种复习。

定义 10.1.1 一个多项式就是一个形如

$$P(x)=a_0x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n,a_0\neq 0$$

的单变量函数。其中系数 $a_0,a_1,\cdots,a_n$ 可以取在全体整数 **Z**，全体有理数 **Q**，全体实数 **R** 或全体复数 **C** 所构成的集合中，$P(x)$ 的(自然)的定义域可以是 **R** 或 **C**。

定义 10.1.2 所有系数在数(环)域 F 中的一元多项式的集合，连同多项式的加法和乘法，称为数(环)域 F 上的一元多项式环，记为 $F[x]$。

多项式具有许多良好的性质，例如多项式是连续的，无限次连续可微的，因此它具有"好"的单变量函数的一切性质，但是它还有比一般的单变量函数"更好"的地方，那就是对多项式可以定义一个叫做次数的概念。利用这一概念，又可以导出许多多项式特有的性质。

定义 10.1.3 设 $P(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ 是一个多项式，那么非负整数 n 就称为这个多项式的次数，记为 $\deg P$。常数多项式的次数是 0，但是为方便起见，规定恒等于 0 的多项式的次数是 -1。

次数有以下性质：

引理 10.1.1

(1) $\deg(P + Q) \leqslant \max(\deg P, \deg Q)$；

(2) $\deg PQ = \deg P + \deg Q$；

(3) $\deg P(Q(x)) = \deg Q(P(x)) = \deg P \cdot \deg Q$。

定义 10.1.4 设 $P(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ 是一个多项式，那么称非负整数 $\deg P + 1$ 是 P 的范数，记为 $N(P)$。

范数有以下性质：

引理 10.1.2

(1) $N(P)$ 是一个整数；

(2) $N(P) = 1$ 的充分必要条件是 P 是非 0 的常数多项式；

(3) $N(P) = 0$ 的充分必要条件是 P 是恒同于 0 的多项式。

多项式又有许多类似于整数的地方，例如可以像整数那样定义整除的概念，因而可以定义因式、倍式、最大公因式、最小公倍式、不可约多项式等概念。

定理 10.1.1

(1) 对于域 F 上的多项式集合 $F[x]$ 中任意两个多项式 $f(x)$ 和 $g(x)$，其中 $g(x) \neq 0$，必存在 $F[x]$ 中的唯一的多项式 $q(x)$ 和 $r(x)$ 使得

$$f(x) = q(x)g(x) + r(x), 0 \leqslant N(r) < N(g)$$

(2) $g(x) \mid f(x)$ 的充分必要条件是在(1)中 $r(x) = 0$。

证明 如果 $f(x) = 0$，那么只要取 $q(x) = r(x) = 0$ 即可。因而以下可设 $f(x)$ 不恒为 0。设 $\deg f = n, \deg g = m$。

当 $n < m$ 时，显然只要取 $q(x) = 0, r(x) = f(x)$ 即可。

当 $n \geqslant m$ 时，设 a, b 分别是 $f(x), g(x)$ 的首项系数(即最高项系数)。那么显然 $\frac{a}{b}x^{n-m}g(x)$ 与 $f(x)$ 的首项相同，因此多项式 $f_1(x) = f(x) - \frac{a}{b}x^{n-m}g(x)$ 的次数要小于 n。

由归纳法假设，对 $f_1(x)$ 和 $g(x)$ 存在 $q_1(x)$ 和 $r_1(x)$ 使得

$$f_1(x) = q_1(x)g(x) + r_1(x), \quad 0 \leqslant N(r_1) < N(g)$$

令 $q(x) = q_1(x) + \frac{a}{b}x^{n-m}, r(x) = r_1(x)$，则

$$f(x) - q(x)g(x) = f(x) - \left(q_1(x) + \frac{a}{b}x^{n-m}\right)g(x) =$$

$$f(x) - q_1(x)g(x) - \frac{a}{b}x^{n-m}g(x) =$$

$$f(x)-\frac{a}{b}x^{n-m}g(x)-q_1(x)g(x)=$$
$$f_1(x)-q_1(x)g(x)=r_1(x)=r(x)$$

因此

$$f(x)=q(x)g(x)+r(x),\quad 0\leqslant N(r)<N(g)$$

因而由数学归纳法就证明了 $q(x),r(x)$ 的存在性。

下面证明唯一性。设还有多项式 $q_1(x)\neq q(x),r_1(x)\neq r(x)$ 使得

$$f(x)=q_1(x)g(x)+r_1(x),\quad 0\leqslant N(r_1)<N(g)$$

成立。那么就有

$$q(x)g(x)+r(x)=q_1(x)g(x)+r_1(x)$$

或

$$(q(x)-q_1(x))g(x)=r_1(x)-r(x)$$

于是由引理 10.1.1 得出

$$\deg g<\deg(q-q_1)+\deg g=\deg(r_1-r)\leqslant\max(\deg r_1,\deg r)<\deg g$$

这是一个矛盾，所得的矛盾说明必须有 $q_1(x)=q(x),r_1(x)=r(x)$。

特别，定理 10.1.1 中令 $g(x)=x-a$，并注意，由于这时 $g(x)$ 的首项系数是 1，$\frac{a}{b}=a$，因而在证明中就不须用到 F 是一个数域的条件，就可以得到

定理 10.1.2 （余式定理）

(1) 设 F 是一个数环，$f(x)$ 是数环 F 上的多项式，那么 $f(x)$ 除以 $x-a$ 所得的余式就是 $f(a)$；

(2) 设 F 是一个数环，$f(x)$ 是数环 F 上的多项式，那么 $x-a\mid f(x)$ 的充分必要条件是 $f(a)=0$。

证明 (1) 由多项式的带余数除法可设

$$f(x)=(x-a)q(x)+c$$

其中 c 是一个常数。在上式中令 $x=a$ 就得出 $f(a)=c$。

(2) 由(1)显然就得出 $x-a\mid f(x)$ 的充分必要条件就是 $c=f(a)=0$，这就证明了定理。

由此定理就得出

定理 10.1.3 设 F 是一个数环，$f(x)\in F[x]$，$x=a$，$a\in F$ 是 $f(x)$ 的根，那么

$$f(x)=(x-a)g(x),g(x)\in F[x]$$

证明 由于 $x=a$，$a\in F$ 是 $f(x)$ 的根，因此 $f(a)=0$，故由定理 10.1.2 即得

$$f(x)=(x-a)q(x),q(x)\in F[x]$$

令 $g(x)=q(x)$ 即得定理 10.1.3。

定理 10.1.4

(1) 设 $f(x)$ 是一个 n 次的复系数多项式,那么 $f(x)$ 最多有 n 个复根;

(2) 设 $f(x)$ 是一个不高于 n 次的复系数多项式,如果 $f(x)$ 在 $n+1$ 个不同的点处都取 0 值,则 $f(x)\equiv 0$;

(3) 设 $f(x)$ 和 $g(x)$ 都是不高于 n 次的复系数多项式,如果 $f(x)$ 和 $g(x)$ 在 $n+1$ 个不同的点处都取到同样的值,则 $f(x)\equiv g(x)$。

证明 (1) 假设 $f(x)$ 有 $n+1$ 个复根 $z_1,z_2,\cdots,z_n,z_{n+1}$,那么反复应用定理 10.1.3 即得

$$f(x)=(x-z_1)(x-z_2)\cdots(x-z_n)(x-z_{n+1})g(x)$$

由上式和引理 10.1.1 就得出

$$n=\deg f=1+1+\cdots+1+1+\deg g>n+1 \quad (\text{式中共有 } n+1 \text{ 个 } 1)$$

这显然是一个矛盾,所得的矛盾说明 $f(x)$ 最多有 n 个复根。

(2) 如果 $f(x)$ 不恒同于 0,那么不高于 n 次的多项式 $f(x)$ 就有 $n+1$ 个根,由(1) 已证,这是不可能的,因此必有 $f(x)\equiv 0$。

(3) 考虑 $h(x)=f(x)-g(x)$,则由引理 10.1.1 可知 $\deg h\leqslant n$,并且 $h(x)$ 在 $n+1$ 个不同的点处都取 0 值。因此由(2) 就得出 $h(x)\equiv 0$,因而有 $f(x)\equiv g(x)$。

习题 10.1

1. (1) 举例说明如果 $f(x)$ 是一个多项式,那么 $f(x)$ 的逆 $\dfrac{1}{f(x)}$ 不一定在整个实数域上有意义。

(2) 举例说明如果 $f(x)$ 是一个多项式,并且 $f(x)$ 的逆 $\dfrac{1}{f(x)}$ 在整个实数域上有意义,$\dfrac{1}{f(x)}$ 也不一定是一个多项式。

2. (1) 证明:$\sin x$,$\cos x$ 都不可能是多项式;

(2) 证明:2^x 不可能是多项式;

(3) 证明:$\log x$ 不可能是多项式;

(4) 证明:$\tan x$ 不可能是多项式;

(5) 证明:$\sqrt[3]{x}$ 不可能是多项式。

3. 证明:周期函数不可能是一个多项式。

4. 找出两个多项式 $p(x)$ 和 $q(x)$,使得 $p(q(x))=q(p(x))$。

5. 设 f,g,h 都是非零多项式,证明:如果 $hf=hg$,那么 $f=g$。

6. (1) 设 $f(x)=ax^2+bx+c$,证明

$$f(1)+f(4)+f(6)+f(7)=f(2)+f(3)+f(5)+f(8)$$

(2) 设 $f(x)$ 是一个三次多项式,证明:可以把$\{1,2,3,\cdots,15,16\}$分成两个集合 A 与 B 使得

$$\sum_{x\in A}f(x)=\sum_{x\in B}f(x)$$

(3) 设 m 是一个正整数,证明:可以把$\{1,2,3,\cdots,2^m,2^{m+1}\}$分成两个集合 A 与 B 使得对任意次数不超过 m 的多项式 $f(x)$ 都有

$$\sum_{x\in A}f(x)=\sum_{x\in B}f(x)$$

7. m,p,q 适合什么条件时,有

(1) $x^2+mx-1\mid x^3+px+q$;

(2) $x^2+mx+1\mid x^4+px^2+q$。

8. 如果 $(x-1)^2\mid Ax^4+Bx^2+1$,求 A,B。

9. 设 $P(x)$ 是一个 n 次多项式,且 $P(k)=\dfrac{k}{1+k}(k=0,1,2,\cdots,n)$,求 $P(n+1)$。

10. 设 $P(x),Q(x),R(x)$ 和 $S(x)$ 都是多项式,且

$$P(x^5)+xQ(x^5)+x^2R(x^5)=(x^4+x^3+x^2+x+1)S(x)$$

证明:$x-1$ 是 $P(x),Q(x),R(x)$ 和 $S(t)$ 的因式。

10.2 代数基本定理和多项式的唯一分解式

在 10.1 中我们已知道数域 F 上的 n 次多项式至多有 n 个因式,并且成立第二带余数除法,由此显然可以得出在 $F[x]$ 中成立欧几里得算法。因此 $F[x]$ 既是一个可分解整环,同时又是一个欧几里得环。由第 9 章的内容可知在 $F[x]$ 中可定义最大公因式,最小公倍式的概念,并且定理 9.4.1 中的 18 条性质和定理 9.4.6 中的 6 条性质以及定理 9.4.7,即唯一分解式定理在 $F[x]$ 中都成立,因此可知 $F[x]$ 中的不可约元就是 $F[x]$ 中的素元素。

这样为具体得出 $Z[x],Q[x],R[x]$ 和 $C[x]$ 中的算术,我们只须确定这些环中的单位元、相伴元和不可约元即可。前两个问题是容易解决的。实际上我们有

定理 10.2.1

(1) $F[x]$ 中的单位元就是 $F[x]$ 中的 0 次多项式,即 F 中的非零常数,因此 $Z[x]$ 的单位元就是任意非零的整数,$Q[x]$ 的单位元就是任意非零的有理数,$R[x]$ 的单位元就是任意非零的实数,$C[x]$ 的单位元就是任意非零的复数;

(2) $F[x]$ 中的相伴元就是 $F[x]$ 中的两个相差一个 F 中非零常数的多项

式；

(3) 在 $F[x]$ 中求两个多项式的最大公因式时，可以把其中任意一个多项式换成它的相伴元，即可对其中任意一个多项式乘以一个 F 中的非零常数。

证明 在欧几里得算法中，当进行到范数为1时，算法就停止了。因此单位元就是欧几里得环中范数为1的元，也就是次数为0的多项式，即 F 中的常数。不过在 $F[x]$ 中有一个特殊情况，那就是作为加法群中的加法单位元的恒同于0的多项式和 F 中作为数的0是无法区分的，因此要特别规定0不能算是通常的常数多项式(这也就是为什么要特别规定0的次数为 -1 的缘故)。而要把它从一般的常数多项式中区分出来。

例 10.2.1 求 $f(x)=x^4+3x^3-x^2-4x-3$ 和 $g(x)=3x^3+10x^2+2x-3$ 的最大公因式，并将它表示为 $f(x)$ 和 $g(x)$ 的线性组合。

解

$$(f,g)=(x^4+3x^3-x^2-4x-3,3x^3+10x^2+2x-3)=$$
$$(3x^4+9x^3-3x^2-12x-9,3x^3+10x^2+2x-3)=$$
$$3x^4+9x^3-3x^2-12x-9=x(3x^3+10x^2+2x-3)+(-x^3-5x^2-9x-9)$$
$$(f,g)=(-x^3-5x^2-9x-9,x^3+10x^2+2x-3)=$$
$$(3x^3+15x^2+27x+27,3x^3+10x^2+2x-3)=$$
$$(5x^2+25x+30,3x^3+10x^2+2x-3)=$$
$$(x^2+5x+6,3x^3+10x^2+2x-3)=$$
$$(x^2+5x+6,-5x^2-16x-3)=$$
$$(x^2+5x+6,5x^2+16x+3)=(x^2+5x+6,-9x-27)=$$
$$(x^2+5x+6,x+3)=(2x+6,x+3)=$$
$$(x+3,x+3)=x+3$$

把上面的式子写成等式就是

$$3f=xg-r_1,r_1=x^3+5x^2+9x+9$$
$$3r_1=g+r_2,r_2=5x^2+25x+30$$
$$g=\frac{3}{5}xr_2-r_3,r_3=5x^2+16x+3$$
$$r_3=r_2-r_4,r_4=9x+27$$
$$(f,g)=\frac{1}{9}r_4$$

由此倒退回去就得到

$$(f,g)=\frac{1}{9}r_4=\frac{1}{9}(r_2-r_3)=\frac{1}{9}\left(r_2+g-\frac{3}{5}xr_2\right)=$$
$$\frac{1}{9}\left(\left(-\frac{3}{5}x+1\right)r_2+g\right)=$$

$$\frac{1}{9}\left(\left(-\frac{3}{5}x+1\right)(3r_1-g)+g\right)=\frac{1}{9}\left(\left(-\frac{9}{5}x+3\right)r_1+\frac{3}{5}xg\right)=$$
$$\frac{1}{3}\left(-\frac{3}{5}x+1\right)r_1+\frac{1}{15}xg=\frac{1}{3}\left(-\frac{3}{5}x+1\right)(xg-3f)+\frac{1}{15}xg=$$
$$\left(\frac{3}{5}x-1\right)f+\left(-\frac{1}{5}x^2+\frac{2}{5}x\right)g$$

在定理 10.1.1 的证明中，我们用到了域中的非零元素都有逆这一性质，因而不适用于多项式环 $Z[x]$，然而上面的例子表明，只要适当修改证明过程，就可以证明在 $Z[x]$ 中同样可以实行欧几里得算法。实际上，设 $f(x),g(x)\in Z[x]$，那么由定理 10.1.1 对作为 $Q[x]$ 中的 $f(x),g(x)$ 成立第二带余数除法和欧几里得算法，然后把这些算法中式子里的分母去掉，就得到相应的 $Z[x]$ 中的式子。由此得到：

定理 10.2.2

(1) 设 $f(x),g(x)\in Z[x]$，那么存在适当的正整数 λ，使得对 $\lambda f(x),g(x)$ 成立第二带余数除法，即存在 $q(x),r(x)\in Z[x]$ 使得

$$\lambda f(x)=q(x)g(x)+r(x),\quad 0\leqslant \deg r<\deg g$$

(2) 对 $f(x),g(x)\in Z[x]$，成立以下形式的欧几里得算法：

$$\lambda_1 f(x)=q_1(x)g(x)+r_1(x),\quad 0\leqslant \deg r_1<\deg g$$
$$\lambda_2 f(x)=q_2(x)r_1(x)+r_2(x),\quad 0\leqslant \deg r_2<\deg r_1$$
$$\vdots$$
$$\lambda_{n-1}r_{n-3}(x)=q_{n-1}(x)r_{n-2}(x)+r_{n-1}(x),\quad 0\leqslant \deg r_{n-1}<\deg r_{n-2}$$
$$\lambda_n r_{n-2}(x)=q_n(x)r_{n-1}(x)+r_n(x),\quad 0\leqslant \deg r_{n-1}<\deg r_n$$
$$\lambda_{n+1}r_{n-1}(x)=q_{n+1}(x)r_n(x)$$

其中 $\lambda_i,i=1,2,\cdots,n+1$ 是正整数，$q_i,i=1,2,\cdots,n+1,r_i,i=1,2,\cdots,n\in Z[x]$。

(3) 对 $f(x),g(x)\in Z[x]$，存在正整数 $k>0$ 和 $\lambda(x),\mu(x)\in Z[x]$，使得

$$k(f,g)=\lambda f+\mu g$$

多项式环虽然有很多类似于整数的性质，但是它和整数的最大区别就是它不仅有一般的可分解整环和欧几里得环的共同性质，还要受系数所在的环或域的性质的影响。但是我们指出，有一个性质是不受影响的，那就是下面的

定理 10.2.3 两个多项式之间的整除关系不因系数域的扩大而改变。

证明 设 f,g 是 $F[x]$ 中的两个多项式，K 是包含 F 的一个较大的数域，即有 $F\subset K$。那么显然 f,g 也是 $K[x]$ 中的多项式。因此如果在 $F[x]$ 中 $g\mid f$，那么当然在 $K[x]$ 中也有 $g\mid f$。如果 $F[x]$ 在 g 中不能整除 f，那么由带余数除法

可知，用 g 除 f 所得的余式 $r \neq 0$。由余式的唯一性可知，在 $K[x]$ 中用 g 除 f 所得的余式仍是 $r \neq 0$，因此在 $K[x]$ 中 g 也不能整除 f。这就证明了定理。

为了确定 $Z[x]$，$Q[x]$，$R[x]$ 和 $C[x]$ 中的不可约因子，我们需要所谓的代数基本定理。这个定理首先是由德国数学家高斯证明的，到目前为止，已出现了多种证明方法，这些方法大体上可以分为拓扑学的、复变函数的和计算方法的三种，但不管哪一种，一般都需要作相当篇幅的准备工作，用到各自领域中的一个"大"的定理。如果我们不先证明这些预备知识就直接引用它们来证代数基本定理，那就和没有证明本质上是一样的。因此本书中不准备这样做。根据最新的资料，我们下面给出的证明虽然也要用到一些复变函数的内容，但都属于本质上仍是微积分的知识。

所谓本质上仍是微积分的知识的意思是，如果你已熟悉了直到二元函数的微分方面的内容，你就会发现，任何一本复变函数的教材在讲到柯西积分之前，在复变中所讲的极限、求导数、微分等内容基本上都是微积分学的简单的推广。直到讲柯西积分才算正式有了复变函数的特点。这表现在，在微积分课程中，一般讲完了一阶导数和微分后，还要将高阶导数和微分，而且关于微分的内容一般不需要和积分联系起来，但是在复变函数中却不是这样，他要先讲完了柯西积分再回过头来再讲高阶的导数和微分。在微积分中，一个一阶可微的函数不一定还可以继续微分和求导，但是在复变函数中，一个函数只要可微，就无限次可微，这就是二者之间的一个重大区别了。而要证明这一性质，必须要用到柯西积分。目前我还没有见到过一本书是可以直接证明这一性质的。所以我们认为，用到复变函数中柯西积分以前的内容虽然在形式上用到了复变函数，但是在本质上仍未超过微积分的内容。

另外，检验一个证明是否真正是简明易懂的标准之一是看你是否能随时将它讲出来，相信下面给出的证明是符合这一标准的。

定义 10.2.1 设 $f(x)$ 是连续函数。如果在 x_0 在的任意小邻域 $(x_0-\delta, x_0+\delta)$ 中都有 $f(x) \leqslant f(x_0)$，则称 $f(x_0)$ 是 $f(x)$ 的一个山峰；如果在 x_0 在的任意小邻域 $(x_0-\delta, x_0+\delta)$ 中都有 $f(x) \geqslant f(x_0)$，则称 $f(x_0)$ 是 $f(x)$ 的一个山谷。

定义 10.2.2 设 $f(z)$ 是一个连续的复变数的实值函数。如果在 z_0 在的任意小邻域 $B(z_0,\delta)$（即以 z_0 为圆心，δ 为半径的一个开圆）中都有 $f(z) \leqslant f(z_0)$，则称 $f(z_0)$ 是 $f(z)$ 的一个山峰；如果在 z_0 在的任意小邻域 $B(z_0,\delta)$ 中都有 $f(z) \geqslant f(z_0)$，则称 $f(z_0)$ 是 $f(z)$ 的一个山谷。

引理 10.2.1（费马定理） 设函数 $f(x)$ 在 x_0 的某一邻域 $(x_0-\delta, x_0+\delta)$ 内有定义，$f(x_0)$ 是 $f(x)$ 的山峰或山谷，$f'(x_0)$ 存在，则必有 $f'(x_0)=0$。

证明 假设 $f'(x_0) \neq 0$，那么必有 $f'(x_0) > 0$ 或 $f'(x_0) < 0$。

如果 $f'(x_0) > 0$,那么由导数的定义就有

$$f'(x_0) = \lim_{x \to x_0} \frac{f(x) - f(x_0)}{x - x_0} > 0$$

于是根据极限的性质就有必存在 x_0 的某一邻域$(x_0 - \delta_1, x_0 + \delta_1) \subset (x_0 - \delta, x_0 + \delta)$ 使得在$(x_0 - \delta_1, x_0 + \delta_1)$ 内成立$\frac{f(x) - f(x_0)}{x - x_0} > 0$,这就说明当 $x > x_0$ 时,$f(x) > f(x_0)$,当 $x < x_0$ 时,$f(x) < f(x_0)$,因此 $f(x_0)$ 不可能是 $f(x)$ 的山峰或山谷。

同理可证如果 $f'(x_0) < 0$,$f(x_0)$ 也不可能是 $f(x)$ 的山峰或山谷。

这就说明必有 $f'(x_0) = 0$。

引理 10.2.2

(1) 设函数 $f(x)$ 在 x_0 的某一邻域$(x_0 - \delta, x_0 + \delta)$ 内有定义,$f(x_0)$ 是 $f(x)$ 的山峰,$f'(x_0)$,$f''(x_0)$ 存在,则必有 $f''(x_0) \leqslant 0$。

(2) 设函数 $f(x)$ 在 x_0 的某一邻域$(x_0 - \delta, x_0 + \delta)$ 内有定义,$f(x_0)$ 是 $f(x)$ 的山谷,$f'(x_0)$,$f''(x_0)$ 存在,则必有 $f''(x_0) \geqslant 0$。

证明 (1) 如果 $f''(x_0) > 0$,那么首先由引理 10.2.1 得出 $f'(x_0) = 0$。再由导数的定义就有

$$f''(x_0) = \lim_{x \to x_0} \frac{f'(x) - f'(x_0)}{x - x_0} = \lim_{x \to x_0} \frac{f'(x)}{x - x_0} > 0$$

于是根据极限的性质就有必存在 x_0 的某一邻域$(x_0 - \delta_1, x_0 + \delta_1) \subset (x_0 - \delta, x_0 + \delta)$ 使得在$(x_0 - \delta_1, x_0 + \delta_1)$ 内成立$\frac{f(x)}{x - x_0} > 0$,这就说明当 $x > x_0$ 时,$f'(x) > 0$,当 $x < x_0$ 时,$f'(x) < 0$。

于是当 $x > x_0$ 时

$$f(x) - f(x_0) = \int_{x_0}^{x} f'(x)\mathrm{d}x > 0$$

当 $x < x_0$ 时,仍有

$$f(x) - f(x_0) = \int_{x_0}^{x} f'(x)\mathrm{d}x = -\int_{x}^{x_0} f(x)\mathrm{d}x > 0$$

这说明 $f(x_0)$ 是 $f(x)$ 的山谷,与假设矛盾,因此必有 $f''(x_0) \leqslant 0$。

(2) 类似于(1) 同理可证。

引理 10.2.3

(1) 设 $w(x, y)$ 是 R^2 中的二次可微的实值函数,$w(x_0, y_0)$ 是 $w(x, y)$ 的山峰,则

$$\Delta w(x_0, y_0) = \frac{\partial^2 w}{\partial x^2}(x_0, y_0) + \frac{\partial^2 w}{\partial y^2}(x_0, y_0) \leqslant 0$$

(2) 设 $w(x,y)$ 是 R^2 中的二次可微的实值函数，$w(x_0,y_0)$ 是 $w(x,y)$ 的山谷，则

$$\Delta w(x_0,y_0) = \frac{\partial^2 w}{\partial x^2}(x_0,y_0) + \frac{\partial^2 w}{\partial y^2}(x_0,y_0) \geqslant 0$$

证明 (1) 考虑两个一元函数 $f(x) = w(x,y_0)$ 和 $g(y) = w(x_0,y)$，那么显然

$$w(x_0,y_0) = f(x_0) = g(y_0)$$

是 $f(x)$ 和 $g(y)$ 的山峰。因此由引理 10.2.2 即得

$$\frac{\partial^2 w}{\partial x^2}(x_0,y_0) = f''(x_0) \leqslant 0, \quad \frac{\partial^2 w}{\partial y^2}(x_0,y_0) = g''(y_0) \leqslant 0$$

因而

$$\Delta w(x_0,y_0) = \frac{\partial^2 w}{\partial x^2}(x_0,y_0) + \frac{\partial^2 w}{\partial y^2}(x_0,y_0) \leqslant 0$$

(2) 类似于(1) 同理可证。

引理 10.2.4 设 $w(x,y)$ 是 $\mathbf{R}^2$ 中的连续的正的实值函数，当 $x^2+y^2 \to \infty$ 时，$w(x,y) \to 0$，那么 $w(x,y)$ 必存在一个最大值 $w(x_0,y_0)$，而且 $w(x_0,y_0)$ 必定是 $w(x,y)$ 的山峰。

证明 (1) 首先，$w(x,y)$ 必有上界 M，否则由于当 $x^2+y^2 \to \infty$ 时，$w(x,y) \to 0$，那么必存在一个以原点为中心，四边平行于坐标轴的正方形 K，使得在 K 之外 $|w(x,y)| \leqslant 1$。因此 $w(x,y)$ 在 K 之外是有上界的，故它只能在 K 内无上界。把 K 用坐标轴划分为 4 个小正方形，那么 $w(x,y)$ 必在某一个小正方形 K_1 内无界，再把 K_1 划分为 4 个小正方形，那么 $w(x,y)$ 又必在某一个小正方形 K_2 内无界，如此进行下去，我们就得到一个正方形的区间套，$w(x,y)$ 在这些正方形上都是无界的。

$$K \supset K_1 \supset K_2 \supset \cdots \supset K_n \supset \cdots$$

并且可使得正方形 K_n 的对角线的长度趋于 0。由区间套定理就可知道必有一个唯一的点 (x_0,y_0) 属于这些正方形，并且 $w(x,y)$ 在 (x_0,y_0) 处无界，因此由连续性可知当 $(x,y) \to (x_0,y_0)$ 时必有 $|w(x,y)| \to \infty$，而这与 $w(x,y)$ 在 R^2 中处处有定义矛盾，故 $w(x,y)$ 必有上界。

(2) 其次，$w(x,y)$ 有上界，因此 $w(x,y)$ 必有上确界 M，我们证明 $w(x,y)$ 必能达到此上确界。假设不然，那么对任意 $(x,y) \in K$，$w(x,y) < M$。令 $v(x,y) = \dfrac{1}{M - w(x,y)}$，那么显然 $v(x,y)$ 在 K 上连续，因而根据(1) 中的证明，$v(x,y)$ 在 K 中必有正的上界 $\dfrac{1}{\mu}$，因而

$$\frac{1}{M-w} = v < \frac{1}{\mu}$$

由此得出

$$M - w > \mu, w < M - \mu < M$$

这说明 $w(x,y)$ 有一个小于 M 的上界，而这与 M 是 $w(x,y)$ 的上确界矛盾，因此 $w(x,y)$ 必能达到它的上确界 M。

(3) 设 $w(x_0,y_0) = M$，那么显然 $w(x_0,y_0)$ 是 $w(x,y)$ 的山峰。

引理 10.2.5 设 $Q(z)$ 是一个允许自变量取复值的复系数非零多项式，那么必存在一个实数 $d > 0$ 具有性质：如果 $Q(a) = 0$，则 $Q(a+d) \neq 0$。

证明 由定理 10.1.4 知 $Q(z)$ 只有有限个根 $z_1, z_2, \cdots, z_n$，因此可定义一个实数

$$0 < d < \min\{|z_i - z_j|, i \neq j\}$$

如果 $Q(a) = 0$，同时又有 $Q(a+d) = 0$，那么由 d 的定义就得出

$$d < |a + d - d| = |d|$$

这是一个矛盾，所得的矛盾就说明 $Q(a+d) \neq 0$。

定义 10.2.3 设 D 是复平面 C 中的一个开子集，一个 D 上的复值函数 $f(z)$ 称为在 D 上是全纯的，如果 $f(z)$ 在 D 的每个点上都是可微的。

仿照单变量的实变函数的相应手段容易证明：

引理 10.2.6

(1) 两个在 D 上全纯的函数的和，差与积仍是全纯的；

(2) 如果 g 在 D 上是全纯的，且对每个 $z \in D, g(z) \neq 0$，那么 $\frac{1}{g}$ 在 D 上是全纯的，且 $\left(\frac{1}{g}\right)' = -\frac{g'}{g^2}$。

定义 10.2.4 设 D 是复平面 C 中的一个开子集，一个 D 上的复值函数 $f(z)$ 称为在 D 上是解析的，如果 $f(z)$ 在 D 的每个点上都是无限次可微的。

仿照单变量的实变函数的相应手段容易证明：

引理 10.2.7 设 $P(z) = a_0z^n + a_1z^{n-1} + \cdots + a_n$ 是复平面 C 上的复系数多项式，那么 $P(z)$ 在全平面上是解析的，且

$$P'(z) = na_0z^{n-1} + (n-1)a_1z^{n-2} + \cdots + a_{n-1}$$

引理 10.2.8 设 $f(z) = u(x,y) + iv(x,y), z = x + iy$ 是定义在 D 上的复变函数，且 $f(z)$ 在 $z_0 = x_0 + iy_0 \in D$ 处可微，则 $u(x,y), v(x,y)$ 在 (x_0,y_0) 点处可微，并且满足柯西 - 黎曼条件。

$$u_x(x_0,y_0) = v_y(x_0,y_0), v_x(x_0,y_0) = -u_y(x_0,y_0)$$

证明 由于 $f(z)$ 在 z_0 处可微，因而导数 $f'(z_0) = a + ib$ 存在。根据可微的定义，就有

$$\Delta f = f'(z_0)\Delta z + \rho(\Delta z)$$

其中 $\rho(\Delta z) = \epsilon_1(\Delta z) + i\epsilon_2(\Delta z)$ 满足当 $\Delta z \to 0$ 时，$\frac{\rho(\Delta z)}{\Delta z} \to 0$。把上式用实数的符号写出来就是

$$\Delta u + i\Delta v = (a + bi)(\Delta x + i\Delta y) + \rho(\Delta z)$$

或

$$\Delta u + i\Delta v = a\Delta x - b\Delta y + i(b\Delta x + a\Delta y) + \rho(\Delta z)$$

比较上式两边的实部和虚部就得出

$$\Delta u = a\Delta x - b\Delta y + \epsilon_1(\Delta z)$$

$$\Delta v = b\Delta x + a\Delta y + \epsilon_2(\Delta z)$$

显然 ϵ_1, ϵ_2 满足条件当 $\Delta z \to 0$ 时，$\frac{\epsilon_1(\Delta z)}{\Delta z} \to 0, \frac{\epsilon_2(\Delta z)}{\Delta z} \to 0$。故 $u(x, y), v(x, y)$ 在 (x_0, y_0) 点处可微，且

$$u_x(x_0, y_0) = v_y(x_0, y_0) = a$$

$$v_x(x_0, y_0) = -u_y(x_0, y_0) = b$$

引理 10.2.9 如果 $f(z)$ 和 $f'(z)$ 在 D 上都是可微的，那么

$$\Delta(|f(z)|^2) = 4|f'(z)|^2$$

此处 Δ 的意义是

$$\Delta w(x, y) = \frac{\partial^2 w}{\partial x^2}(x, y) + \frac{\partial^2 w}{\partial y^2}(x, y)$$

证明 设 $f(z) = u(x, y) + iv(x, y)$，那么 $|f(z)|^2 = u^2 + v^2$。由此得出如果 $w = |f(z)|^2$，那么

$$w_x = 2uu_x + 2vv_x, w_{xx} = 2uu_{xx} + 2u_x^2 + 2vv_{xx} + 2v_x^2$$

类似的

$$w_{yy} = 2uu_{yy} + 2u_y^2 + 2vv_{yy} + 2v_y^2$$

由引理 10.2.8 知 $u(x, y), v(x, y)$ 在 D 上满足柯西 - 黎曼条件

$$u_x = v_y, v_x = -u_y$$

因此

$$f'(z) = u_x + iv_x = v_y - iu_y$$

$$\Delta u = u_{xx} + u_{yy} = (u_x)_x + (u_y)_y = (v_y)_x + (-v_x)_y = 0$$

同理 $\Delta v = 0$。故

$$\begin{aligned}\Delta w = w_{xx} + w_{yy} = {} & 2uu_{xx} + 2u_x^2 + 2vv_{xx} + 2v_x^2 + 2uu_{yy} + 2u_y^2 + 2vv_{yy} + 2v_y^2 = \\ & 2u(u_{xx} + u_{yy}) + 2v(v_{xx} + v_{yy}) + 2u_x^2 + 2v_x^2 + 2u_y^2 + 2v_y^2 = \\ & 2u\Delta u + 2v\Delta v + 2|f'(z)|^2 + 2|f'(z)|^2 = 4|f'(z)|^2\end{aligned}$$

定理 10.2.4(代数基本定理) 每个不恒同于常数的复系数多项式在复数域中都必有一个根。

证明 设 $p(z)$ 是一个不恒同于常数的复系数多项式，则 $p'(z)$ 是一个不恒同于0的多项式。因此由引理10.2.5得出必存在一个实数 $d>0$ 具有性质：如果 $p'(z)=0$，那么就有 $p'(z+d)\neq 0$。

假如不存在任何复数 z_0 使得 $p(z_0)=0$，那么函数 $f(z)=\frac{1}{p(z)}$ 和 $f(z+d)$ 在复平面 C 上都是全纯的，因此函数

$$w(x,y)=|f(z)|^2+|f(z+d)|^2$$

恒取正值且在 C 上连续并具有连续的二阶导数。并且显然当 $x^2+y^2\to\infty$ 时，$w(x,y)\to 0$。故由引理10.2.4可知 $w(x,y)$ 必存在一个最大值 $w(x_0,y_0)$，而且 $w(x_0,y_0)$ 必定是 $w(x,y)$ 的山峰。因此由引理10.2.3和引理10.2.9得出

$$0\leqslant 4(|f'(z_0)|^2+|f'(z_0+d)|^2)=\Delta w(x_0,y_0)\leqslant 0$$

其中 $z_0=x_0+\mathrm{i}y_0$，由此得出

$$f'(z_0)=f'(z_0+d)=0$$

然而由于

$$f'(z_0)=-\frac{p'(z_0)}{p^2(z_0)},\quad f'(z_0+d)=-\frac{p'(z_0+d)}{p^2(z_0+d)}$$

因此从上面的式子就可以得出

$$p'(z_0)=0,\quad p'(z_0+d)=0$$

这与 d 的性质矛盾，所得的矛盾就说明了必存在复数 z_0 使得 $p(z_0)=0$。

由代数基本定理和定理10.1.2，定理10.1.3就得出 $C[x]$ 中所有次数大于1的多项式全是可约的，这也就是说 $C[x]$ 中的不可约因子只有一次多项式，但是这个一次因子是可以相差一个单位数，在这里也就是复数的。不过如果我们把 x 之前的系数统统都提出去，那这个一次因子就完全确定了。由于我们现在已经完全确定了 $C[x]$ 中的不可约因子，因此根据第九章9.4中的整除性理论就可得出 $C[x]$ 的唯一分解定理如下：

定理10.2.5（复系数多项式的唯一分解定理） 每个不不恒同于常数的复系数多项式在复数域中在不计次序的意义下都可以唯一地分解成形如

$$f(z)=a_0(x-\alpha_1)^{k_1}(x-\alpha_2)^{k_2}\cdots(x-\alpha_s)^{k_s}$$

的一次因式的乘积。其中 $\alpha_1,\alpha_2,\cdots,\alpha_s$ 是不同的复数，a_0 也是复数。$k_1,k_2,\cdots,k_s$ 是正整数。

利用代数基本定理和定理10.1.3就可得出：

定理10.2.6 每个 n 次的复系数多项式恰有 n 个复根（重根按重数计算）。

下面来确定 $R[x]$ 中的不可约因子。我们有：

引理10.2.10 如果 α 是实系数多项式 $f(x)$ 的复根，那么 α 的共轭复数 $\bar{\alpha}$ 也是 $f(x)$ 的复根。

证明　设 $f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n$，其中 $a_0,a_1,\cdots,a_n$ 都是实数。那么由假设

$$a_0\alpha^n+a_1\alpha^{n-1}+\cdots+a_n=0$$

在上式两边取共轭，并利用实数的共轭仍是它自己这一事实就得出

$$a_0\bar{\alpha}^n+a_1\bar{\alpha}^{n-1}+\cdots+a_n=0$$

这就证明了引理。

由此引理立刻可以得出一个大家都很熟悉的结果

引理 10.2.11　奇数次的实系数多项式至少有一个实根。

证明　由引理 10.2.10 可知实系数多项式的复根都是成对出现的，所以如果一个奇数次多项式完全没有实根的话，那它就要有偶数个根，然而根据定理 10.2.5 又有奇数次多项式恰有奇数个根，这就矛盾了，因此就可知一个奇数次多项式至少要有一个实根。

引理 10.2.12　设 ax^2+bx+c 是一个判别式小于 0 的实二次多项式，又设 α 是此二次多项式的一个根。如果 α 是实系数多项式 $f(x)$ 的根，那么 $ax^2+bx+c\mid f(x)$。

证明　根据引理 10.2.10 可知 $\bar{\alpha}$ 也是 ax^2+bx+c 和 $f(x)$ 的根，因此可把 ax^2+bx+c 分解成形式

$$ax^2+bx+c=a(x-\alpha)(x-\bar{\alpha})$$

由于 α 和 $\bar{\alpha}$ 都是的 $f(x)$ 根，因此我们有

$$x-\alpha\mid f(x),\ x-\bar{\alpha}\mid f(x)$$

容易证明在 $C[x]$ 中 $x-\alpha$ 和 $x-\bar{\alpha}$ 是既约的因而也是互素的(由于 $C[x]$ 既是可分解环又是欧几里得环，因此这两个概念是一致的)，因而根据我们在第 9 章 9.4 中的整除性理论就可得出

$$ax^2+bx+c=a(x-\alpha)(x-\bar{\alpha})\mid f(x)$$

上面这个证明是利用了整环的整除性理论，由于我们在第三章和第九章中两次系统地讨论了这个理论，所以我们认为读者应该是已经很熟悉这个理论了。对不熟悉这个理论的读者，我们用带余数除法也可以证明。即根据带余数除法可设

$$f(x)=q(x)(ax^2+bc+c)+kx+h$$

把 $x=\alpha$ 和 $x=\bar{\alpha}$ 分别代入上式就可得出一个关于 k,h 的二元一次方程组

$$\alpha k+h=0$$
$$\bar{\alpha}k+h=0$$

这个方程组的系数行列式是

$$\begin{vmatrix}\alpha & 1\\ \bar{\alpha} & 1\end{vmatrix}=\alpha-\bar{\alpha}$$

由于我们假设 ax^2+bx+c 是一个判别式小于 0 的实二次多项式，因此 $\alpha,\bar{\alpha}$ 都不是实根，故 $\alpha-\bar{\alpha}\neq 0$（否则 $\alpha=\bar{\alpha}$ 将是实数）。因此上面那个二元一次方程组必有唯一解 $k=h=0$，因此根据余式定理就证明了必有 $ax^2+bx+c\mid f(x)$。

引理 10.2.13 $R[x]$ 中的不可约因子的次数至多是 2。

证明 设 $f(x)$ 是一个 3 次或 3 次以上的多项式。如果 $f(x)$ 有实根，那么显然 $f(x)$ 可分出一个一次因子，因而不可能是不可约多项式。如果 $f(x)$ 没有实根，那么它必有一对共轭复根 $\alpha,\bar{\alpha}$，因而根据引理 10.2.12 可知实系数多项式 x^2+px+q 可整除 $f(x)$，其中 $p=-(\alpha+\bar{\alpha})$，$q=\alpha\bar{\alpha}$，因而 $f(x)$ 也不可能是不可约多项式。这就证明了引理。

有这个引理就得出

引理 10.2.14 $R[x]$ 中的不可约因子只有一次多项式和判别式小于 0 的二次多项式。

由此就可得出 $R[x]$ 中的唯一分解定理为

定理 10.2.7（实系数多项式的唯一分解定理） 每个不恒同于常数的实系数多项式在实数域中在不计次序的意义下都可以唯一地分解成形如

$$f(z)=a_0(x-\alpha_1)^{k_1}(x-\alpha_2)^{k_2}\cdots(x-\alpha_s)^{k_s}\cdot(x^2+p_1x+q_1)^{h_1}(x^2+p_2x+q_2)^{h_2}\cdots(x^2+p_rx+q_r)^{h_r}$$

的因式的乘积。其中 $\alpha_1,\alpha_2,\cdots,\alpha_s$ 是不同的实数，$p_1,p_2,\cdots,p_r,q_1,q_2,\cdots,q_r$ 都是实数，a_0 也是实数。$k_1,k_2,\cdots,k_s,h_1,h_2,\cdots,h_r$ 是正整数，并且其中每个二次多项式的判别式都小于 0。

至于 $Z[x]$ 和 $Q[x]$ 中的不可约多项式，我们在定理 4.4.4 中已经指出，在有理数范围内，存在着次数任意高的不可约多项式。尽管我们有像爱森斯坦判别法这样的充分性条件，但是并没有一般的充分必要条件。但是由于有定理 4.4.1，即设 $f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n$ 是整系数多项式。那么如果有理数 $\frac{p}{q}$ 是 $f(x)$ 的根，其中 p,q 是互素的整数，$q\neq 0$；则必有 $p\mid a_n$，$q\mid a_0$。所以可以知道，对一个具体给定了系数的 $Z[x]$ 和 $Q[x]$ 中的多项式，我们是必可在有限的步骤内判定它是否是一个不可约多项式的。

利用代数基本定理，我们还可以得出一个关于非负的实系数多项式的表示式的定理。

定理 10.2.8 设 $f(x)$ 是一个非负的实系数多项式，则 $f(x)$ 一定可表示成两个实系数多项式的平方和的形式。

证明 由于 $f(x)$ 是非负的，因此它的一次因子的方次一定是一个偶数。因而当把 $f(x)$ 的平方因子都提出去后，所余的因式就不可能再有实根了。也就是说我们可把 $f(x)$ 表示成为

$$f(x) = d^2(x)g(x)$$

的形式,其中 $d(x)$,$g(x)$ 都是实系数多项式,且 $g(x)$ 没有实根。

由引理10.2.10可知 $g(x)$ 的复根是成对出现的,因此可把 $g(x)$ 表示成下述形式

$$g(x) = (x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n)(x - \bar{\alpha}_1)(x - \bar{\alpha}_2)\cdots(x - \bar{\alpha}_n) = h(x)\overline{h(x)}$$

设 $h(x) = P(x) + \mathrm{i}Q(x)$,那么 $\overline{h(x)} = P(x) - \mathrm{i}Q(x)$,其中 $P(x)$,$Q(x)$ 都是实系数多项式,因此

$$f(x) = d^2(x)g(x) = d^2(x)(P(x) + \mathrm{i}Q(x))(P(x) - \mathrm{i}Q(x)) = d^2(x)(P^2(x) + Q^2(x)) = (\mathrm{d}P)^2 + (\mathrm{d}Q)^2$$

是两个实系数多项式的平方和。

这个定理中的平方和一般也是无法精确地求出来的,但是即使是近似的表达式,有时也可以转化为精确的表示式,因此还是有实用价值的。

例 10.2.2 证明:$f(x) = x^6 - 10x^5 + 40x^4 - 82x^3 + 91x^2 - 52x + 13$ 是正定的。

证明 我们先利用定理10.2.7给出 $f(x)$ 的近似表示式。

在 Matlab 命令窗口中键入以下命令:

```
Format long
p = [1,  10,40,  82,91,  52,13];
roots(p)
```

并回车即可得到如下数据:

2.795 261 884 992 54 + 0.159 616 959 862 75i

2.795 261 884 992 54 − 0.159 616 959 862 75i

1.606 963 891 846 08 + 0.746 125 431 245 58i

1.606 963 891 846 08 − 0.746 125 431 245 58i

0.597 774 223 161 38 + 0.413 491 528 617 14i

0.597 774 223 161 38 − 0.413 491 528 617 14i

这些数据即是 $f(x)$ 的复根的近似值。因此

$$f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)(x - \bar{\alpha}_1)(x - \bar{\alpha}_2)(x - \bar{\alpha}_3)$$

其中

$$\alpha_1 = 2.795\,261\,884\,992\,54 + 0.159\,616\,959\,862\,75\mathrm{i}$$

$$\alpha_2 = 1.606\,963\,891\,846\,08 + 0.746\,125\,431\,245\,58\mathrm{i}$$

$$\alpha_3 = 0.597\,774\,223\,161\,38 + 0.413\,491\,528\,617\,14\mathrm{i}$$

因而

$$h(x) = x^3 - (\alpha_1 + \alpha_2 + \alpha_3)x^2 + (\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1)x - \alpha_1\alpha_2\alpha_3 =$$

$$x^3-(5.000\,000\,000\,000\,000+1.319\,233\,919\,725\,47\mathrm{i})x^2+$$
$$(6.629\,810\,932\,522\,90+4.703\,827\,190\,421\,97\mathrm{i})x-$$
$$(1.645\,496\,955\,253\,96+3.208\,167\,665\,545\,24\mathrm{i})$$

于是

$$P(x)=x^3-5x^2+6.629\,810\,932\,522\,90x-1.645\,496\,955\,253\,96$$
$$Q(x)=-(1.319\,233\,919\,725\,47x^2-4.703\,827\,190\,421\,97x+3.208\,167\,665\,545\,24)$$

而

$$f(x)=P^2(x)+Q^2(x)$$

这样我们就得到了 $f(x)$ 的正定的近似表示式。

虽然这只是一个近似的表示式，但是它还是给我们不少有用的线索。首先，如果我们要想精确地求出这一表示式，我们可从上式得知，它的形式是

$$f(x)=(x^3-px^2+qx-r)^2+(\alpha x^2-\beta x+\gamma)^2=$$
$$x^6-2px^5+(p^2+2q+\beta^2)x^4-(2pq+2r+2\alpha\beta)x^3+$$
$$(q^2+2pr+\alpha^2+2\alpha\gamma)x^2-(2qr+2\beta\gamma)x+r^2+\gamma^2$$

对照上式和 $f(x)$ 的系数即可得出 $p,q,r,\alpha,\beta,\gamma$ 必须满足下述的方程组

$$2p=10,\quad p=5$$
$$p^2+2q+\beta^2=40$$
$$2pq+2r+2\alpha\beta=82,pq+r+\alpha\beta=41$$
$$q^2+2pr+\alpha^2+2\alpha\gamma=91$$
$$2qr+2\beta\gamma=52,qr+\beta\gamma=26$$
$$r^2+\gamma^2=13$$

上面这个方程组当然是不可能精确地解出来的，因为你消元后，他肯定就化成原来的 6 次方程。但是我们现在已经有了这个方程组的近似解。于是就可考虑先拿几个近似解作出发点，看是否能精确地解出其他解。

通过观察上面的方程组，我们发现，如果假定 α 和 β 为已知，并且选取四次方和奇数次方的系数作为方程组(因为已经假定两个未知数为已知，方程组的方程就需要减少两个才能保持适定)。就可将其余的未知数精确地解出来。这样虽然总体上说，我们得到的仍是一组近似解，但只要是这组近似解满足下述两个不等式

$$q^2+2pr+\alpha^2+2\alpha\gamma<91$$
$$r^2+\gamma^2<13$$

则由于这两个不等式原来都是偶数次方的系数，因此我们就可把 $f(x)$ 精确地表示成一些偶数次方的和，因而现在已是精确地证明了 $f(x)$ 的正定性。

从直觉上来说，我们相信，只要取足够精确的不足近似值或过剩近似值，上述要求是一定可以达到的。事实上，经过试验，也确实如此。至于如何取近似值，

利用我们已经讲过的连分数理论是不难获得合适的近似值的。于是最后我们获得通过一组近似解所得的精确表示式为

$$f(x)=(x^3-5x^2+qx-r)^2+(\alpha x^2-\beta x+\gamma)^2+hx^2+k$$

其中

$$q=\frac{2\ 494\ 350\ 015}{371\ 226\ 752},\quad q=\frac{2\ 494\ 350\ 015}{371\ 226\ 752},\quad r=\frac{38\ 606\ 917\ 420\ 590\ 974}{22\ 222\ 817\ 897\ 050\ 489}$$

$$\alpha=\frac{17\ 025}{13\ 624},\quad \beta=\frac{2\ 745\ 875\ 683\ 028\ 574\ 226\ 589}{605\ 527\ 342\ 058\ 831\ 724\ 272},\quad \gamma=\frac{10\ 603}{3\ 356}$$

$$h=\frac{1\ 141\ 986\ 350\ 028\ 202\ 042\ 589\ 996\ 820\ 690\ 333\ 145\ 829\ 281\ 965\ 578\ 537}{57\ 100\ 346\ 932\ 656\ 156\ 469\ 418\ 716\ 190\ 689\ 196\ 597\ 799\ 700\ 929\ 560\ 576}$$

$$k=\frac{11\ 272\ 010\ 677\ 261\ 141\ 998\ 525\ 534\ 793\ 470\ 503}{5\ 562\ 143\ 116\ 860\ 505\ 295\ 352\ 570\ 239\ 976\ 723\ 095\ 056}$$

至于如何求出实根乃至复根的近似值,有多少个实根,如何估计实根的界限等问题,在一门叫做“计算数学”的学科中专家们做着专门的研究,本书就不讨论这些问题了。

利用实系数多项式的分解式我们还可以得出把有理分式化简为部分分式的定理。

引理 10.2.15 设$\dfrac{f(x)}{g(x)}$是整环 F 上的有理分式(即 $f(x),g(x)\in F[x]$),$g(x)=g_1(x)g_2(x)$,其中 $g_1(x),g_2(x)$ 既约(即$(g_1(x),g_2(x))=\varepsilon$,$\varepsilon$ 是 F 中的单位元),则$\dfrac{f(x)}{g(x)}$可以表示为 $a\dfrac{f(x)}{g(x)}=\dfrac{c_1u(x)}{b_1g_1(x)}+\dfrac{c_2v(x)}{b_2g_2(x)}$ 的形式,其中 a,$b_1,b_2,c_1,c_2\in F$。

证明 前面已证多项式环既是可分解环又是欧几里得环,因此在 $F[x]$ 中既约的多项式就是互素的多项式,这也就是说必存在两个多项式 $u_1(x)$,$v_1(x)\in F[x]$ 使得

$$a(u_1g_1+u_2g_2)=\varepsilon$$

因而

$$\frac{af}{bg}=\frac{\varepsilon f(u_1g_1+v_1g_2)}{bg_1g_2}=\frac{\varepsilon fv_1}{bg_1}+\frac{\varepsilon fu_1}{bg_2}=\frac{c_1u}{b_1g_1}+\frac{c_2v}{b_2g_2}$$

这就证明了引理。

引理 10.2.16 设 $p(x)$ 是整环 F 上的不可约多项式,则有理分式$\dfrac{f(x)}{p^m(x)}$,$m\geqslant 1$ 可表示成

$$a_0\frac{f(x)}{p^m(x)}=b_0f_0(x)+\frac{c_1f_1(x)}{b_1p(x)}+\frac{c_2f_2(x)}{b_2p^2(x)}+\cdots+\frac{c_mf_m(x)}{b_mp^m(x)}$$

$$\deg f_i<\deg p,\ i=1,2,\cdots,m$$

的形式，其中 $a_0, b_0, b_1, \cdots, b_m, c_1, \cdots, c_m \in F$。

证明 用 $p(x)$ 去除 $f(x)$，由整环中的带余数除法得

$$\lambda_1 f(x) = \mu_1 q_1(x) p(x) + f_m(x)$$

再用 $p(x)$ 去除 $q_1(x)$，得

$$\lambda_2 q_1(x) = \mu_2 q_2(x) p(x) + f_{m-1}(x), \cdots$$

如此下去，直到

$$\lambda_m q_{m-1}(x) = \mu_m f_0(x) p(x) + f_{m-1}(x)$$

把上面的式子合起来就有

$$a_0 f(x) = b_0 f_0(x) p^m(x) + b_1 f_1(x) p^{m-1}(x) + \cdots + b_{m-1} f_{m-1}(x) p(x) + b_m f_m(x)$$

由此就得出引理。

通常把形如$\dfrac{u(x)}{p^m(x)}$，$\deg u < \operatorname{dep} p$ 的分式称为简单分式。利用这一术语就可把有理分式的分解叙述成

定理 10.2.8 环 F 上的每个有理分式都可以表示成一个多项式与一些简单分式的线性组合。

证明 由于环 F 上的每个不恒等于常数的多项式 $g(x)$ 都可以分解成

$$g(x) = c p_1^{r_1}(x) p_2^{r_2}(x) \cdots p_s^{r_s}(x)$$

所以应用引理 10.2.15 和引理 10.2.16 就得到定理。

在具体应用上述定理时，由于定理已保证了分解的存在性，所以可以直接假定上述分解式成立，再利用待定系数法之类的方法即可得出所要的分解式。

例 10.2.3 在 $Z[x]$ 中把$\dfrac{4x^2+4x-11}{(2x-1)(2x+3)(2x-5)}$分解成部分分式。

解 首先在 $Q[x]$ 中将此分式分解得到

$$\frac{4x^2+4x-11}{(2x-1)(2x+3)(2x-5)} = \frac{\frac{1}{2}x^2+\frac{1}{2}x-\frac{1}{8}}{\left(x-\frac{1}{2}\right)\left(x+\frac{3}{2}\right)\left(x-\frac{5}{2}\right)} = \frac{A}{x-\frac{1}{2}} + \frac{B}{x+\frac{3}{2}} + \frac{C}{x-\frac{5}{2}}$$

把分母去掉，就得到一个恒等式

$$\frac{1}{2}x^2+\frac{1}{2}x-\frac{1}{8} = A\left(x+\frac{3}{2}\right)\left(x-\frac{5}{2}\right) + B\left(x-\frac{1}{2}\right)\left(x-\frac{5}{2}\right) + C\left(x-\frac{1}{2}\right)\left(x+\frac{3}{2}\right)$$

在此恒等式中分别令 $x = \frac{1}{2}, -\frac{3}{2}, \frac{5}{2}$ 即得 $A = \frac{1}{4}, B = -\frac{1}{8}, C = \frac{3}{3}$。由此即

得到在 $Q[x]$ 中的分解式如下

$$\frac{4x^2+4x-11}{(2x-1)(2x+3)(2x-5)}=\frac{\frac{1}{4}}{x-\frac{1}{2}}-\frac{\frac{1}{8}}{x+\frac{3}{2}}+\frac{\frac{3}{8}}{x-\frac{5}{2}}$$

现在把所得的分解式中分子分母中的数的分母去掉，就得到在 $Z[x]$ 中的分解式如下

$$\frac{4x^2+4x-11}{(2x-1)(2x+3)(2x-5)}=\frac{1}{2(2x-1)}-\frac{1}{4(2x+3)}+\frac{3}{4(2x-5)}$$

例 10.2.4 在 $R[x]$ 中把分式$\frac{1}{x^2(1+x^2)^2}$分解成部分分式。

解

$$\frac{1}{x^2(1+x^2)^2}=\frac{(1+x^2)-1}{x^2(1+x^2)^2}=\frac{1}{x^2(1+x^2)}-\frac{1}{(1+x^2)^2}=$$

$$\frac{(1+x^2)-1}{x^2(1+x^2)}-\frac{1}{(1+x^2)^2}=$$

$$\frac{1}{x^2}-\frac{1}{1+x^2}-\frac{1}{(1+x^2)^2}$$

把分式分解成部分分式的一个直接目的是计算此分式的积分。然而在积分的计算过程中，人们发现，实际上为计算有理分式的积分，可直接将其积分的有理部分求出来，因而可大大简化计算。这称为分离积分的有理部分。

设有即约的真分式$\frac{P}{Q}$，又设它的分母已分解成素因式

$$Q(x)=(x-a)^k\cdots(x^2+px+q)^m$$

于是这个分式的积分可以表示成分式

$$\frac{A_1}{x-a}+\frac{A_2}{(x-a)^2}+\cdots+\frac{A_k}{(x-a)^k}$$

和

$$\frac{M_1x+N_1}{x^2+px+q}+\frac{M_2x+N_2}{(x^2+px+q)^2}+\cdots+\frac{M_mx+N_m}{(x^2+px+q)^m}$$

的积分的和。如果 k(或 m) 大于 1，则由积分公式可知，除$\frac{A_1}{x-a}$ 和$\frac{M_1x+N_1}{x^2+px+q}$之外，其余各项的积分仍得到有理分式，因此最后的积分的形式为

$$\int\frac{P(x)}{Q(x)}\mathrm{d}x=\frac{P_1(x)}{Q_1(x)}+\int\frac{P_2(x)}{Q_2(x)}\mathrm{d}x$$

其中$\frac{P_1(x)}{Q_1(x)}$就是积分$\int\frac{P(x)}{Q(x)}\mathrm{d}x$ 的有理部分。由于它是由上面所分离出的一部分有理部分相加而得到的，所以它首先是一个真分式，而它的分母有分解式

$$Q_1(x) = (x-a)^{k-1}\cdots(x^2+px+q)^{m-1}\cdots$$

至于留在积分号里面的分式，由于它们本来就是真分式的一部分，所以也是真分式，并且

$$Q_2(x) = (x-a)\cdots(x^2+px+q)\cdots$$

显然 $Q = Q_1Q_2$。公式

$$\int \frac{P(x)}{Q(x)}\mathrm{d}x = \frac{P_1(x)}{Q_1(x)} + \int \frac{P_2(x)}{Q_2(x)}\mathrm{d}x$$

称为奥斯特洛格拉德斯基公式。取微分后，可把它表示成等价的形式

$$\frac{P}{Q} = \left(\frac{P_1}{Q_1}\right)' + \frac{P_2}{Q_2}$$

在实际计算时，如果已知 Q 的分解式，那么根据上面所讲的法则，Q_1，Q_2 就可以立刻写出。但是即使不知道 Q 的分解式，Q_1 也可以确定。这是由于 Q' 包含 Q 的所有素因式（请自己验证），只是其中素因式的方次数少 1，所以 Q_1 其实就是 Q' 和 Q 的最大公因式，因而可由 Q' 和 Q 定出。一旦知道了 Q_1，由 $Q = Q_1Q_2$ 例用除法即可求出 Q_2。求出 Q_1，Q_2 后，P_1，P_2 就可用待定系数法求出。

例 10.2.5 分离积分 $\int \frac{4x^4+4x^3+16x^2+12x+8}{(x+1)^2(x^2+1)^2}\mathrm{d}x$ 的有理部分。

解 $$Q_1 = Q_2 = (x+1)(x^2+1) = x^3+x^2+x+1$$

因此可设

$$\frac{4x^4+4x^3+16x^2+12x+8}{(x^3+x^2+x+1)^2} = \left(\frac{ax^2+bx+c}{x^3+x^2+x+1}\right)' + \frac{dx^2+ex+f}{x^3+x^2+x+1}$$

由此

$$\begin{aligned}4x^4+4x^3+16x^2+12x+8 = {} & (2ax+b)(x^3+x^2+x+1) - \\ & (ax^2+bx+c)(3x+2x+1) + \\ & (dx^2+ex+f)(x^3+x^2+x+1)\end{aligned}$$

把右边展开，对照两边同类项的系数就得出

x^5：$d = 0$ （因此在下面的计算中一律把 d 换成 0）

x^4：$-a+e=4$

x^3：$-2b+e+f=4$

x^2：$a-b-3c+e+f=16, a=-1, b=1, c=-4$

x^1：$2a-2c+e+f=12, d=0, e=3, f=3$

x^0：$b-c+f=8$

于是得到

$$\int \frac{4x^4+4x^3+16x^2+12x+8}{(x+1)^2(x^2+1)^2}\mathrm{d}x = -\frac{x^2-x+4}{x^3+x^2+x+1} + 3\int\frac{\mathrm{d}x}{x^2+1}$$

例 10.2.6 分离积分 $\int \frac{2x^4-4x^3+24x^2-40x+20}{(x-1)(x^2-2x+2)^3}\mathrm{d}x$ 的有理部分。

解 $Q_1=(x^2-2x+2)^2, Q_2=(x-1)(x^2-2x+2)$

于是

$$\frac{2x^4-4x^3+24x^2-40x+20}{(x-1)(x^2-2x+2)^3}=\left(\frac{ax^3+bx^2+cx+d}{(x^2-2x+2)^2}\right)'+\frac{e}{x-1}+\frac{fx+g}{x^2-2x+2}$$

由此得出

$$\begin{aligned}2x^4-4x^3+24x^2-40x+20=&(3ax^2+2bx+c)(x^2-2x+2)(x-1)-\\&(ax^3+bx^2+cx+d)\cdot 2(2x-2)(x-1)+\\&(fx+g)(x-1)(x^2-2x+2)^2\end{aligned}$$

与例 10.2.5 类似,可导出方程组

$$\begin{aligned}&x^6: e+f=0\\&x^5: -a-6e-5f+g=0\\&x^4: -a-2b+18e+12f-5g=2\\&x^3: 8a+2b-3c-32e-16f+12g=-4\\&x^2: -6a+4b+5c-4d+36e+12f-16g=24\\&x^1: -4b+8d-24e-4f+12g=-40\\&x^0: -2c-4d+8e-4g=20\end{aligned}$$

由此解出 $a=2, b=-6, c=8, d=-9, e=2, f=-2, g=4$,因而

$$\frac{2x^4-4x^3+24x^2-40x+20}{(x-1)(x^2-2x+2)^3}=\left(\frac{2x^3-6x^2+8x-9}{(x^2-2x+2)^2}\right)'+\frac{2}{x-1}-\frac{2x-4}{x^2-2x+2}$$

习题 10.2

1. 设 $f(z)=u(x,y)+\mathrm{i}v(x,y), z=x+\mathrm{i}y$ 是定义在 D 上的复变函数,证明:如果 $u(x,y), v(x,y)$ 在 (x_0,y_0) 点处可微,并且满足柯西 - 黎曼条件

$$u_x(x_0,y_0)=v_y(x_0,y_0), v_x(x_0,y_0)=-u_y(x_0,y_0)$$

则 $f(z)$ 在 $z_0=x_0+\mathrm{i}y_0\in D$ 处可微。

2. (1) 验证 $f(z)=\sqrt{|xy|}$ 在 $z=0$ 处满足柯西 - 黎曼条件;

(2) 证明:$f(z)$ 在 $z=0$ 处不可导;

(3)(1) 与(2) 是否矛盾?

3. 求 $f(x)$ 和 $g(x)$ 的最大公因式

(1) $f(x)=x^4+x^3-3x^2-4x-1, g(x)=x^3+x^2-x-1$;

(2) $f(x)=x^4-4x^3+1, g(x)=x^3-3x^2+1$;

(3) $f(x)=x^4-10x^2+1, g(x)=x^4-4\sqrt{2}x^3+6x^2+4\sqrt{2}x+1$。

4. 求 $u(x), v(x)$ 使得 $u(x)f(x)+v(x)g(x)=(f(x),g(x))$。

(1)$f(x)=x^4+2x^3-x^2-4x-2, g(x)=x^4+x^3-x^2-2x-2$;

(2)$f(x)=4x^4-2x^3-16x^2+5x+9, g(x)=2x^3-x^2-5x+4$;

(3)$f(x)=3x^3-2x^2+x+2, g(x)=x^2-x-1$;

(4)$f(x)=x^4-x^3-4x^2+4x+1, g(x)=x^2-x-1$;

(5)$f(x)=x^4, g(x)=(1-x)^4$。

5.证明:如果 $f(x),g(x)$ 不全为零,且 $u(x)f(x)+v(x)g(x)=(f(x),g(x))$,则$(u(x),v(x))=1$。

6.证明:如果$\frac{f(x)}{(f(x),g(x))}$,$\frac{g(x)}{(f(x),g(x))}$的次数都大于零,就可选出 $u(x),v(x)$ 使得

$$u(x)f(x)+v(x)g(x)=(f(x),g(x))$$

且

$$\deg u(x)<\deg\frac{g(x)}{(f(x),g(x))},\deg v(x)<\deg\frac{f(x)}{(f(x),g(x))}$$

7.设 $f(x)=x^3+(1+t)x^2+2x+2u, g(x)=x^3+tx^2+u$ 的最大公因式是一个二次多项式,求 t,u 的值。

8.设 $p(x)$ 是次数大于零的多项式。证明:如果对于任何多项式 $f(x)$, $g(x)$,由 $p(x)\mid f(x)g(x)$ 可以得出 $p(x)\mid f(x)$ 或 $p(x)\mid g(x)$,则 $p(x)$ 必是不可约多项式。

9.证明:次数大于零的多项式是一个不可约多项式的方幂的充分必要条件是对任意的多项式必有$(f(x),g(x))=1$ 或者对某一个正整数 $m,f(x)\mid g(x)^m$。

10.证明:次数大于零的多项式是一个不可约多项式的方幂的充分必要条件是对任意的多项式 $g(x),h(x)$,由 $f(x)\mid g(x)h(x)$ 必可推出有 $f(x)\mid g(x)$ 或者对某一个正整数 $m,f(x)\mid h(x)^m$。

11.在实数域上,把下列分式分解成部分分式

(1) $\frac{3x+4}{x^2+3x+2}$　　(2) $\frac{x^2-1}{x^4+3x^2-4}$

(3) $\frac{3x-7}{(x-2)^3}$　　(4) $\frac{1}{(x^4-1)^2}$

(5) $\frac{x^6}{(x+1)(x^2+1)^2}$

12.分出下列分式积分的有理部分

(1) $\frac{x}{(x-1)^2(x+1)^3}$　　(2) $\frac{1}{(x^3+1)^2}$

(3) $\frac{1}{(x^2+1)^3}$　　(4) $\frac{x^2}{(x^2+2x+2)^2}$

(5) $\dfrac{1}{(x^4+1)^2}$　　(6) $\dfrac{x^2+3x-2}{(x-1)(x^2+x+1)^2}$

(7) $\dfrac{1}{(x^4-1)^3}$　　(8) $\dfrac{x^2+1}{(x^4+x^2+1)^2}$

(9) $\dfrac{1}{(x^3+x+1)^3}$　　(10) $\dfrac{4x^5-1}{(x^5+x+1)^2}$

13. 证明：$y = 2x^4 - 1\cdot 2x^3 - 2x^2 + 1$ 是正定的。

13. 证明：$y = x^4 - 6x^2 + 4x + 16\cdot 25$ 是正定的。

14. 证明：$y = x^6 - x^5 + x^4 - x^3 + x^2 - x + 1$ 是正定的。

15. 证明：$y = x^6 - 7x^5 + 21x^4 - 35x^3 + 35x^2 - 21x + 7$ 是正定的。

10.3　重根和公根

在本节中，均设所讨论的多项式是在实数域上或复数域上定义的。

定义 10.3.1　如果在多项式 $f(x)$ 的唯一分解式中不可约多项式 $p(x)$ 的指数为 k，$k > 1$，则称 $p(x)$ 为多项式 $f(x)$ 的 k 重因式。否则称 $p(x)$ 为 $f(x)$ 的单因式。(不考虑 $k = 0$ 的情况，因为这时 $p(x)$ 根本不是 $f(x)$ 的因式)

引理 10.3.1　不可约多项式 $p(x)$ 是多项式 $f(x)$ 的 k 重因式的充分必要条件是 $p^k(x) \mid f(x)$ 而 $p^{k+1}(x) \mid f(x)$。

证明　充分性：如果 $p^k(x) \mid f(x)$ 而 $p^{k+1}(x) \mid f(x)$，那么因为 $p(x)$ 是不可约多项式，因此在 $f(x)$ 的唯一分解式中必含有 $p(x)$，设 $p(x)$ 的指数为 r，那么显然，$k \leqslant r < k+1$，因而只能有 $r = k$，这就证明了 $p(x)$ 是多项式 $f(x)$ 的 k 重因式。

必要性：反之，设 $p(x)$ 是多项式 $f(x)$ 的 k 重因式，那么在 $f(x)$ 的唯一分解式中 $p(x)$ 的指数为 k，那么由分解式的唯一性就显然得出 $p^k(x) \mid f(x)$ 而 $p^{k+1}(x) \mid f(x)$。

为了判断多项式 $f(x)$ 是否有重因式，我们引进下述概念。

定义 10.3.2　设多项式 $f(x)$ 为 $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$，则多项式 $a_0nx^{n-1} + a_1(n-1)x^{n-2} + \cdots + a_{n-1}$ 称为 $f(x)$ 的微商，记为 $f'(x)$。

定义 10.3.3　$f'(x)$ 称为 $f(x)$ 的一阶微商，$f'(x)$ 的微商称为 $f(x)$ 的二阶微商，记为 $f''(x)$。一般的，如果已经定义了 $f(x)$ 的 k 阶微商，并把它记为 $f^{(k)}(x)$，那么我们定义 $f^{(k)}(x)$ 的微商为 $f(x)$ 的 $k+1$ 阶微商，并把它记为 $f^{(k+1)}(x)$。

微商和导数这些概念显然是来源于数学分析。不过数学家们也是有各自的研究领域的，有些数学家愿意尽可能地用本领域的范围内的知识来解决本领域

的问题。(当然也有些数学家不在乎用什么范围内的知识) 我觉得这也不是什么怪癖。因为如果本来可以用一个系统内的工具去解决问题,你却要突然从另一个系统内去取一个工具来用,就显得有点乱,我不是认为不可以这样做,而是觉得,如果不是非这样不可,就不必这样做(除非你还有其他特别的原因,例如证明特别简单之类)。我们通过定义多项式的微商,可以从形式上完全避免用数学分析的方法来讨论问题,但仍能够利用数学分析中的概念和结果。

引理 10.3.2 多项式的微商有以下性质:

(1)$(f(x)+g(x))'=f'(x)+g'(x)$;

(2)$(cf(x))'=cf'(x)$;

(3)$(f(x)g(x))'=f'(x)g(x)+f(x)g'(x)$;

(4)$(f^m(x))'=mf^{m-1}(x)f'(x)$。

定理 10.3.1 如果不可约多项式 $p(x)$ 是 $f(x)$ 的 $k(k>1)$ 重因式,那么 $p(x)$ 就是 $f(x)$ 的微商 $f'(x)$ 的 $k-1$ 重因式。

证明 由于 $p(x)$ 是 $f(x)$ 的 k 重因式,因此根据定义就可把 $f(x)$ 写成 $f(x)=p^k(x)g(x)$ 的形式,其中 $p(x)$ 不能整除 $g(x)$。因此

$$f'(x)=kp^{k-1}(x)p'(x)g(x)+p^k(x)g'(x)=$$
$$p^{k-1}(x)(kg(x)p'(x)+p(x)g'(x))$$

这就说明 $p^{k-1}(x)\mid f'(x)$。令 $h(x)=kg(x)p'(x)+p(x)g'(x)$,那么 $p(x)$ 整除 $p(x)g'(x)$ 项,但是由于 $p(x)$ 不能整除 $g(x)$,$p(x)$ 不能整除 $p'(x)$(因为 $p'(x)$ 的次数比 $p(x)$ 的次数小 1),所以 $p(x)$ 不能整除 $kg(x)p'(x)$(否则由于 $p(x)$ 是不可约多项式,将得出 $p(x)\mid g(x)$ 或 $p(x)\mid p'(x)$)。这就说明 $p^k(k)\nmid f'(x)$,因此 $p(x)$ 是 $f'(x)$ 的 $k-1$ 重因式。

由此定理可以得出

定理 10.3.2

(1) 如果不可约多项式 $p(x)$ 是 $f(x)$ 的 k 重因式,那么 $p(x)$ 是

$$f(x),f'(x),\cdots,f^{(k-1)}(x)$$

的因式,但不是 $f^{(k)}(x)$ 的因式;

(2) 不可约多项式 $p(x)$ 是 $f(x)$ 的重因式的充分必要条件是 $p(x)$ 是 $f(x)$ 和 $f'(x)$ 公因式;

(3) 多项式 $f(x)$ 没有重因式的的充分必要条件是 $f(x)$ 和 $f'(x)$ 互素。

证明 (1) 由定理 10.3.1 得出 $p(x)$ 是 $f'(x)$ 的 $k-1$ 重因式,$f''(x)$ 的 $k-2$ 重因式,…,$f^{(k-1)}(x)$ 的 1 重因式,这就证明了 $p(x)$ 是 $f(x),f'(x),\cdots,f^{(k-1)}(x)$ 的因式。

$p(x)$ 是 $f^{(k-1)}(x)$ 的 1 重因式即 $p(x)$ 是 $f^{(k-1)}(x)$ 的单因式,因此 $f^{(k-1)}(x)$ 可写成

$$f^{(k-1)}(x) = p(x)g(x)$$

的形式，其中 $p(x)$ 不能整除 $g(x)$。因此

$$f^{(k)}(x) = p'(x)g(x) + p(x)g'(x)$$

$p(x)$ 整除 $p(x)g'(x)$ 项，但是由于 $p(x)$ 不能整除 $g(x)$，$p(x)$ 不能整除 $p'(x)$，所以 $p(x) \nmid p'(x)g(x)$，这就说明 $p^k(x) \nmid f^{(k)}(x)$。

(2) 由定理 10.3.1 知 $f(x)$ 的重因式必须是 $f'(x)$ 的因式，反之不可约多项式 $p(x)$ 如果是 $f'(x)$ 的因式，那么由(1) 中最后的证明可知 $p(x)$ 不可能是 $f(x)$ 的单因式(用同样的方法也可证明 $p(x)$ 根本不是 $f(x)$ 的因式)，因此必是 $f(x)$ 的重因式。

(3) 由(2) 即可得出。

本来按照重因式的定义，我们需要把 $f(x)$ 的唯一分解式求出来才能知道一个不可约多项式 $p(x)$ 是不是它的重因式。但是由于并没有一般地去求一个多项式的唯一分解式的方法，所以用这个方法去判断一个不可约多项式 $p(x)$ 是不是 $f(x)$ 的重因式是行不通的。然而定理 10.3.2 却告诉我们，这个问题可以通过一种初等的代数运算，也就是辗转相除法来判断，不仅如此，利用辗转相除法还可以把多项式的各个不同重数的因式分离出来。

由余数定理我们知道 α 是 $f(x)$ 的根的充分必要条件是 $x-\alpha \mid f(x)$。由此我们可以给重根一个严格的定义。

定义 10.3.4 如果 $x-\alpha$ 是 $f(x)$ 的 k 重因式，则称 α 是 $f(x)$ 的 k 重根。当 $k=1$ 时，α 称为单根；当 $k>1$ 时，α 称为重根。

上面我们已经得出了不可约多项式 $p(x)$ 是 $f(x)$ 的重因式的充分必要条件是 $p(x)$ 是 $f(x)$ 和 $f'(x)$ 公因式；这就提出了求 $f(x)$ 和 $f'(x)$ 公因式或公根的问题，虽然这一问题已可由辗转相除法解决，但是我们现在更一般地提出两个完全无关的多项式

$$f(x) = a_0x^m + a_1x^{m-1} + \cdots + a_m, \quad m > 0$$

和

$$g(x) = b_0x^n + b_1x^{n-1} + \cdots + b_n, \quad n > 0$$

有无公根的问题，并且希望给出一个判据(因为多项式完全由它的系数确定，因此这个问题也完全由 $f(x)$ 和 $g(x)$ 的系数所确定)。

在第五章中，我们已经定义了结式的概念，并证明结式完全由 $f(x)$ 和 $g(x)$ 的系数所确定，定义 5.3.9 设 $a_0 \neq 0$，$f(x) = a_0x^m + a_1x^{m-1} + \cdots + a_m$ 的所有根是 $\alpha_1, \alpha_2, \cdots, \alpha_m$，$b_0 \neq 0$，$g(x) = b_0x^n + b_1x^{n-1} + \cdots + b_n$ 的所有根是 $\beta_1, \beta_2, \cdots, \beta_m$，则称

$$R(f,g) = a_0^n b_0^m \prod_{i=1}^{m} \prod_{j=1}^{n} (\alpha_i - \beta_j)$$

为多项式 $f(x)$ 和 $g(x)$ 的结式。

定义 10.3.5

(1) $R(f,g) = a_0^n g(\alpha_1)g(\alpha_2)\cdots g(\alpha_m) = b_0^m f(\beta_1)f(\beta_2)\cdots f(\beta_m)$;

(2) $R(f,g)$ 可由 $f(x)$ 和 $g(x)$ 的系数表出;

(3) 多项式 $f(x)$ 和 $g(x)$ 有公共根的充分必要条件是 $R(f,g) = 0$。

我们现在的目的是求出用 $f(x)$ 和 $g(x)$ 的系数表出的结式的公式。

定理 10.3.3

$$R(f,g) = \Delta(m,n) = \begin{vmatrix} a_0 a_1 \cdots a_m & & & \\ & a_0 a_1 \cdots a_m & & \\ & & \cdots & \\ & & & a_0 a_1 \cdots a_m \\ b_0 b_1 \cdots b_n & & & \\ & b_0 b_1 \cdots b_n & & \\ & & \cdots & \\ & & & b_0 b_1 \cdots b_n \end{vmatrix}$$

(上面的行列式前 n 行由 $f(x)$ 的系数组成,后 m 行由 $g(x)$ 的系数组成)

证明 对 $f(x)$ 的次数实行数学归纳法。

当 $m = 1$ 时

$$f(x) = a_0 x + a_1, a_0 \neq 0$$
$$g(x) = b_0 x^n + b_1 x^{n-1} + \cdots + b_n, b_0 \neq 0$$

这时 $f(x)$ 的唯一的根是 $\alpha = -\dfrac{a_1}{a_0}$,而

$$\Delta(1,n) = \begin{vmatrix} a_0 a_1 & & & \\ & a_0 a_1 & & \\ & & \ddots & \\ & & & a_0 a_1 \\ b_0 b_1 & \cdots & & b_{n-1} b_n \end{vmatrix}$$

用 α 乘上面的行列式的第一列后加到第二列上,再用 α 乘所得的行列式的第二列后加到第三列上,…,最后再用 α 乘所得的行列式的第 n 列后加到第 $n+1$ 列上。那么所得的行列式中的元素 a_1 都被消去(也就是原来是 a_1 的地方现在都是 0)。而最后一行的元素依次等于

$$b_0, b_0\alpha + b_1, \cdots, b_0\alpha^{n-1} + b_1\alpha^{n-2} + \cdots + b_{n-1},$$
$$b_0\alpha^n + b_1\alpha^{n-1} + \cdots + b_n = g(\alpha)$$

也就是说行列式 $\Delta(1,n)$ 所对应的矩阵变成了一个下三角阵,因而 $\Delta(1,n)$ 的值就等于它的对角线元素的乘积。

$$\Delta(1,n) = \begin{vmatrix} a_0 & & & & \\ & a_0 & & & \\ & & \ddots & & \\ & & & a_0 & \\ b_0 & b_0\alpha + b_1 & \cdots & & g(\alpha) \end{vmatrix} = a_0^n g(\alpha) = R(f,g)$$

因此定理中的公式对 $m = 1$ 的情况成立。

现在假设定理中的公式对 $m = k$ 的情况成立。那么当 $m = k + 1$ 时

$$f(x) = a_0x^{k+1} + a_1x^k + \cdots + a_{k+1}$$

设 $f(x) = a_0x^{k+1} + a_1x^k + \cdots + a_{k+1}$ 的根是 $\alpha_1,\alpha_2,\cdots,\alpha_k,\alpha$，那么又可设 $f(x) = (x-\alpha)\bar{f}(x)$，$\bar{f}(x) = a_0x^k + c_1x^{k-1} + \cdots + c_k$。显然 $\bar{f}(x)$ 的根是 $\alpha_1,\alpha_2,\cdots,\alpha_k$。比较 $f(x) = a_0x^{k+1} + a_1x^k + \cdots + a_{k+1}$ 和 $f(x) = (x-\alpha)\bar{f}(x)$，$\bar{f}(x) = a_0x^k + c_1x^{k-1} + \cdots + c_k$，这两种 $f(x)$ 的表示式的系数就可得到

$$a_1 = c_1 - a_0\alpha, a_2 = c_2 - c_1\alpha, \cdots, a_k = c_k - c_{k-1}\alpha, a_{k+1} = -c_k\alpha$$

于是

$$\Delta(k+1,n) = \begin{vmatrix} a_0 & c_1 - a_0\alpha \cdots c_k - c_{k-1}\alpha & -c_k\alpha & & \\ & a_0 & c_1 - a_0\alpha \cdots c_k - c_{k-1}\alpha & -c_k\alpha & \\ & & \cdots & & \\ & & a_0 & c_1 - a_0\alpha \cdots c_k - c_{k-1}\alpha & -c_k\alpha \\ b_0 & b_1 \cdots b_n & & & \\ & b_0 & b_1 \cdots b_n & & \\ & & \cdots & & \\ & & b_0 & b_1 \cdots b_n & \end{vmatrix}$$

用 α 乘上面的行列式的第一列后加到第二列上，再用 α 乘所得的行列式的第二列后加到第三列上，…，最后再用 α 乘所得的行列式的第 $n+k$ 列后加到第 $n+k+1$ 列上，并且注意 $b_0\alpha^n + b_1\alpha^{n-1} + \cdots + b_n = g(\alpha)$，我们就得到

$$\Delta(k+1,n) = \begin{vmatrix} a_0 & c_1 & c_2 \cdots & c_k & & & \\ & a_0 & c_1 & c_2 \cdots & c_k & & \\ & & & \cdots & & & \\ & & a_0 & c_1 & c_2 \cdots & c_k & \\ b_0 & b_0\alpha + b_1 \cdots & g(\alpha) & \alpha g(\alpha) \cdots & \alpha^{k-1}g(\alpha) & \alpha^k g(\alpha) & \\ & b_0 & b_0\alpha + b_1 \cdots & g(\alpha) & \alpha g(\alpha) \cdots & \alpha^{k-2}g(\alpha) & \alpha^{k-1}g(\alpha) \\ & & & & \cdots & & \\ & & b_0 & b_0\alpha + b_1 \cdots & & \cdots & g(\alpha) \end{vmatrix}$$

再用 $-\alpha$ 乘第 $n+2$ 行加到第 $n+1$ 行上，用 $-\alpha$ 乘第 $n+3$ 行加到第 $n+2$ 行上，…，最后用 $-\alpha$ 乘第 $n+k+1$ 行加到第 $n+k$ 行上，那么 $\Delta(k+1,n)$ 就成为

$$\Delta(k+1,n)=\begin{vmatrix} a_0\ c_1\cdots\ c_k & & & \\ & a_0\ c_1\cdots\ c_k & & \\ & & \cdots & \\ & & a_0\ c_1\cdots\ c_k & \\ b_0\ b_1\cdots\ b_n & & & \\ & b_0\ b_1\cdots\ b_n & & \\ & & \cdots & \\ & & b_0\ b_1\cdots\ b_n & \\ & & & b_0\ b_0\alpha+b_1\cdots\ g(\alpha) \end{vmatrix}$$

把上面的行列式按最后一列展开（注意在最后一列中，只有最后一行的元素 $g(\alpha)$ 不是 0，其余各行的元素都是 0）就得到

$$\Delta(k+1,n)=(-1)^{k+1+n+k+1+n}g(\alpha)M=g(\alpha)M$$

这里 M 是上面的行列式中位于左上角的 $(n+k)\times(n+k)$ 个元素组成的行列式，经过观察可以发现，M 正好就是由 $\bar{f}(x)$ 和 $g(x)$ 的系数组成的行列式 $\overline{\Delta}(k,n)$。而按照归纳法假设有

$$\overline{\Delta}(k,n)=R(\bar{f},g)=a_0^n g(\alpha_1)g(\alpha_2)\cdots g(\alpha_k)$$

因此

$$\Delta(k+1,n)=g(\alpha)M=g(\alpha)\overline{\Delta}(k,n)=$$
$$a_0^n g(\alpha)g(\alpha_1)g(\alpha_2)\cdots g(\alpha_k)=R(f,g)$$

这就是说，定理中的公式对 $m=k+1$ 的情况也成立，因而我们用数学归纳法就证明了定理。

定理 10.3.4 结式有以下性质：

(1) $R(f,g)=(-1)^{mn}R(g,f)$；

(2) $R(f,g_1g_2)=R(f,g_1)R(f,g_2)$，$R(f_1f_2,g)=R(f_1,g)R(f_2,g)$；

(3) $R(f,cg)=c^mR(f,g)$，其中 c 是一个常数，m 是 $f(x)$ 的次数；$R(cf,g)=c^nR(f,g)$，其中 c 是一个常数，n 是 $g(x)$ 的次数；

(4) 设 $g(x)$ 的次数为 n，根为 $\beta_1,\beta_2,\cdots,\beta_n$。如果 $\lambda f(x)=g(x)q(x)+r(x)$，则

$$R(g,f)=\frac{1}{\lambda^n}R(g,r)$$

$$R(f,g)=\frac{1}{\lambda^n}R(r,g)$$

证明　(1) 设 $a_0 \neq 0, f(x) = a_0x^m + a_1x^{m-1} + \cdots + a_m$ 的所有根是 $\alpha_1, \alpha_2, \cdots, \alpha_m, b_0 \neq 0, g(x) = b_0x^n + b_1x^{n-1} + \cdots + b_n$ 的所有根是 $\beta_1, \beta_2, \cdots, \beta_n$，则

$$R(f,g) = a_0^n b_0^m \prod_{i=1}^{m} \prod_{j=1}^{n} (\alpha_i - \beta_j)$$

上面的连乘号之后共有 mn 个括弧(因为每一个 α_i 要与 n 个 β_j 搭配，而共有 m 个 α_i)，因此

$$R(f,g) = a_0^n b_0^m \prod_{i=1}^{m} \prod_{j=1}^{n} (\alpha_i - \beta_j) = (-1)^{mn} a_0^n b_0^m \prod_{j=1}^{n} \prod_{i=1}^{m} (\beta_j - \alpha_i) = (-1)^{mn} R(g,f)$$

(2) 设 $f(x), g_1(x)$ 和 $g_2(x)$ 的次数分别为 m, r, s，且设 $f(x)$ 的首项系数为 a_0，根为 $\alpha_1, \alpha_2, \cdots, \alpha_m$，则由定理 5.3.5 得出

$$R(f, g_1g_2) = a_0^{r+s} g_1(\alpha_1) g_2(\alpha_1) g_1(\alpha_2) g_2(\alpha_2) \cdots g_1(\alpha_m) g_2(\alpha_m) = a_0^r g_1(\alpha_1) g_1(\alpha_2) \cdots g_1(\alpha_m) a_0^s g_2(\alpha_1) g_2(\alpha_2) \cdots g_2(\alpha_m) = R(f, g_1) R(f, g_2)$$

另一个式子同理可证。

(3) 在(2) 的证明中令 $g_1(x) \equiv c$ 即可。另一个式子同理可证。

(4) 设 $g(x)$ 的次数为 n，首项系数为 b_0，根为 $\beta_1, \beta_2, \cdots, \beta_n$，则

$$R(g,f) = \frac{1}{\lambda^n} R(g, \lambda f) = \frac{b_0^m}{\lambda^n} \lambda f(\beta_1) \lambda f(\beta_2) \cdots \lambda f(\beta_n) = \frac{b_0^m}{\lambda^n} (qg + r)(\beta_1)(qg + r)(\beta_2) \cdots (qg + r)(\beta_n) = \frac{b_0^m}{\lambda^n} r(\beta_1) r(\beta_2) \cdots r(\beta_n) = \frac{1}{\lambda^n} R(g, r)$$

我们在第五章中还定义了一个叫做判别式的概念。

定义 5.3.8　设 $f(x) = a_0x^m + a_1x^{m-1} + \cdots + a_m$ 的所有根是 $\alpha_1, \alpha_2, \cdots, \alpha_m$，则称

$$D(f) = a_0^{2(m-1)} \prod_{i<j} (\alpha_i - \alpha_j)^2$$

为 $f(x) = a_0x^m + a_1x^{m-1} + \cdots + a_m$ 的判别式。

那时我们要根据定义和根与系数的关系去计算判别式，还是比较麻烦的。现在我们来看一下，是否能用多项式的系数直接来表示判别式。

定理 10.3.5　判别式有如下性质：

(1) $D(f) = (-1)^{\frac{m(m-1)}{2}} \frac{1}{a_0} R(f, f')$；

(2) $D(f)$ 是 $f(x)$ 的系数的整系数多项式；

(3) $D(fg) = R^2(f,g) D(f) D(g)$。

证明 (1) 设 $f(x)=a_0x^m+a_1x^{m-1}+\cdots+a_m$ 的所有根是 $\alpha_1,\alpha_2,\cdots,\alpha_m$，则

$$R(f,f')=a_0^{m-1}f'(\alpha_1)f'(\alpha_2)\cdots f'(\alpha_m)$$

由于

$$f(x)=a_0(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_m)$$

因此 $f'(x)$ 可写成

$$f'(x)=a_0\sum_{k=1}^{m}(x-\alpha_1)\cdots(x-\alpha_{k-1})(x-\alpha_{k+1})\cdots(x-\alpha_m)$$

于是

$$R(f,f')=a_0^{m-1}f'(\alpha_1)f'(\alpha_2)\cdots f'(\alpha_m)=$$
$$a_0^{2m-1}f'(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)\cdots(\alpha_1-\alpha_m)(\alpha_2-\alpha_1)(\alpha_2-$$
$$\alpha_3)\cdots(\alpha_2-\alpha_m)\cdots(\alpha_m-\alpha_1)(\alpha_m-\alpha_2)\cdots(\alpha_m-\alpha_{m-1})$$

在上面的乘积中，对于任意一对不考虑次序关系的指数 i,j，都出现两个与之相应的因子 $\alpha_i-\alpha_j$ 和 $\alpha_j-\alpha_i$，它们的乘积等于 $-(\alpha_i-\alpha_j)^2$。由于上面的乘积中带括弧的项共有 m 行，每行有 $m-1$ 个括弧，因此共有 $\frac{m(m-1)}{2}$ 个满足条件 $n\geqslant i>j\geqslant 1$ 的指标对子，因而

$$R(f,f')=(-1)^{\frac{m(m-1)}{2}}a_0a_0^{2(m-1)}\prod_{n\geqslant i>j\geqslant 1}(\alpha_i-\alpha_j)^2=(-1)^{\frac{m(m-1)}{2}}a_0D(f)$$

由此就得出

$$D(f)=(-1)^{\frac{m(m-1)}{2}}\frac{1}{a_0}R(f,f')$$

(2) $D(f)$ 中只有一个在分母中的字母，就是 a_0，根据 $R(f,f')$ 的定义可知，在 $R(f,f')$ 的第一列中共有两个 a_0，其余的元素都是零，因此根据行列式的性质，我们可以把 $R(f,f')$ 第一列中的 a_0 提出来，行列式的符号不变，而提出 a_0 后，行列式中的元素显然都是 1 或 $f(x)$ 的系数和 $f'(x)$ 的系数的整系数多项式，因而 $\frac{1}{a_0}R(f,f')$ 仍是 $f(x)$ 的系数的整系数多项式，这就证明了(2) 的结论。

(3) 设 $f(x)=a_0x^m+a_1x^{m-1}+\cdots+a_m$，$f(x)$ 的所有根为 $\alpha_1,\alpha_2,\cdots,\alpha_m$，$g(x)=b_0x^n+b_1x^{n-1}+\cdots+b_n$，$g(x)$ 的所有根为 $\beta_1,\beta_2,\cdots,\beta_n$，那么由(1) 已证的式子和定理 10.3.4(4) 中的公式就得到

$$D(fg)=(-1)^{\frac{(m+n)(m+n-1)}{2}}\frac{1}{a_0b_0}R(fg,(fg)')=$$
$$(-1)^{\frac{(m+n)(m+n-1)}{2}}\frac{1}{a_0b_0}R(fg,f'g+fg')=$$
$$(-1)^{\frac{(m+n)(m+n-1)}{2}}\frac{1}{a_0b_0}R(f,f'g+fg')R(g,f'g+fg')=$$

$$(-1)^{\frac{(m+n)(m+n-1)}{2}}\frac{1}{a_0b_0}R(f,f'g)R(g,fg')=$$
$$(-1)^{\frac{(m+n)(m+n-1)}{2}}\frac{1}{a_0b_0}R(f,f')R(f,g)R(g,f)R(g,g')=$$
$$(-1)^{\frac{(m+n)(m+n-1)}{2}}\frac{1}{a_0b_0}(-1)^{\frac{m(m-1)}{2}}a_0(-1)^{\frac{n(n-1)}{2}}\cdot$$
$$b_0(-1)^{mn}R^2(f,g)D(f)D(g)=$$
$$(-1)^{(m+n)(m+n-1)}R^2(f,g)D(f)D(g)=R^2(f,g)D(f)D(g)$$

利用判别式的性质,可以得出

定理 10.3.6

(1) 设 $f(x)$ 为实系数多项式,$D(f)$ 是 $f(x)$ 的判别式,那么

当 $D(f)<0$ 时,方程 $f(x)=0$ 无重根,且有奇数对共轭复根;

当 $D(f)=0$ 时,方程 $f(x)=0$ 有重根;

当 $D(f)>0$ 时,方程 $f(x)=0$ 无重根,且有偶数对共轭复根。

(2) 设 $f(x)$ 是三次多项式,则

当 $D(f)<0$ 时,方程 $f(x)=0$ 有一个实根和一对共轭复根;

当 $D(f)=0$ 时,方程 $f(x)=0$ 有重根;

当 $D(f)>0$ 时,方程 $f(x)=0$ 有三个不同的实根。

(3) 设 $f(x)$ 是四次多项式,则

当 $D(f)<0$ 时,方程 $f(x)=0$ 有两个不同的实根和一对共轭复根;

当 $D(f)=0$ 时,方程 $f(x)=0$ 有重根;

当 $D(f)>0$ 时,方程 $f(x)=0$ 有四个不同的实根或两对共轭复根。

证明 (1) 首先写出一次多项式的判别式,设 $f(x)=a_0x+a_1$,次数是 1,那么 $f'(x)=a_0$,次数是 0。于是根据结式的定义,$R(f,f')$ 是一个 $1+0$ 阶行列式,且 $f(x)$ 的系数出现 0 行(也就是根本不出现),$f'(x)$ 的系数出现 1 行,因而

$$R(f,f')=|a_0|=a_0$$

$$D(f)=(-1)^{\frac{1(1-1)}{2}}\frac{1}{a_0}R(f,f')=\frac{1}{a_0}a_0=1$$

所以实系数的一次多项式的判别式恒等于 1。

在第五章中,我们已求出二次多项式 $a_0x^2+a_1x+a_2$ 的判别式是 $a_1^2-4a_0a_2$,并且从中学就知道,如果二次多项式的根是一对共轭复根,则它的判别式就是一个负数。

现在我们来证明(1) 的结论。

根据判别式的定义显然可知 $D(f)=0$ 的充分必要条件是 $f(x)$ 有重根。

如果 $D(f)\neq 0$,那么 $f(x)$ 的根都是单根。由于 $f(x)$ 是实系数多项式,所以它的复根是成对出现的。把 $f(x)$ 的每一对共轭复根凑成一对,就可得到一个二

次多项式，它的判别式是一个负数，于是我们可把 $f(x)$ 分解为以下形式

$$f(x) = a_0 p_1 p_2 \cdots p_r q_1 q_2 \cdots q_s$$

其中，$p_i, i = 1,2,\cdots,r$ 都是实系数一次多项式，$q_i, i = 1,2,\cdots,s$ 都是实系数二次多项式。且 $p_1, p_2, \cdots, p_r, q_1, q_2, \cdots, q_s$ 两两无公根，$q_1, q_2, \cdots, q_s$ 的判别式都是负数。

由定理 10.3.5 中的公式 $D(fg) = R^2(f,g)D(f)D(g)$ 可得

$$D(f) = R^2 D(p_1)D(p_2)\cdots D(p_r)D(q_1)D(q_2)\cdots D(q_s) = R^2 D(q_1)D(q_2)\cdots D(q_s)$$

其中，R 是一些结式的乘积。由于 $p_1, p_2, \cdots, p_r, q_1, q_2, \cdots, q_s$ 两两无公根，所以这些结式都不等于0。这就是说 $D(f)$ 的符号由 $f(x)$ 的共轭复根的对数确定，当 $f(x)$ 的共轭复根的对数是奇数时，$D(f) < 0$，当 $f(x)$ 的共轭复根的对数是偶数时，$D(f) > 0$，并且反过来也成立。这就证明了(1) 的结论。

(2)，(3) 由于三次多项式最多只能有一对共轭复根，四次多项式最多只能有两对共轭复根，因此根据(1) 就容易得出(2)，(3) 的结论。

习题 10.3

1. 证明：如果 $f(x), g(x)$ 互素，则 $f(x^m), g(x^m)$ 也互素。

2. 证明：$x^n + ax^{n-m} + b$ 不可能有重数大于 2 的非零根。

3. 证明：$1 + x + \frac{x^2}{2!} + \cdots + \frac{x^n}{n!}$ 没有重根。

4. 证明：如果 α 是 $f'''(x)$ 的 k 重根，则 α 是 $g(x) = \frac{x-\alpha}{2}[f'(x) + f'(\alpha)] - f(x) + f(\alpha)$ 的 $k+3$ 重根。

5. 证明：α 是 $f(x)$ 的 k 重根的充分必要条件是

$$f(\alpha) = f'(\alpha) = \cdots = f^{(k-1)}(\alpha) = 0, f^{(k)}(\alpha) \neq 0$$

6. 举例说明命题“如果 α 是 $f'(x)$ 的 k 重根，则 α 是 $f(x)$ 的 $k+1$ 重根”不成立。

7. 判别 $x^5 - 5x^4 + 7x^3 - 2x^2 + 4x - 8$ 有没有重因式。

8. 证明：如果 $(x-1) \mid f(x^n)$，则 $(x^n - 1) \mid f(x^n)$。

9. 证明：如果 $(x^2 + x + 1) \mid f_1(x^3) + xf_2(x^3)$，则 $(x-1) \mid f_1(x)$，$(x-1) \mid f_2(x)$。

10. 证明：如果 $f(x) \mid f(x^n)$，则 $f(x)$ 的根只能是零或单位根。

多项式的应用

第十一章

11.1 动力系统奇点的线性稳定性的代数判据

考虑 n 维动力系统

$$\frac{\mathrm{d}X}{\mathrm{d}t}=F(X)$$

并设 X_0 是此系统的奇点或平衡点，即设 $f(X_0)=0$。又设 A 是此系统的线性部分的系数矩阵，即设

$$A=\left.\frac{\partial F}{\partial X}\right|_{X=X_0}$$

而 $f(\lambda)$ 是 A 的特征多项式。那么在常微分方程理论中已经证明了：X_0 是线性稳定的充分必要条件是 $f(\lambda)$ 的所有的根都具有负实部。

所谓 $f(\lambda)$ 的所有的根都具有负实部的意思并不是指它的所有的根都是复根（事实上，由于我们现在考虑的是实系数的微分方程，因此当 $f(\lambda)$ 的次数是奇数时，$f(\lambda)$ 的所有的根也不可能都是复的），而是指，当把 $f(\lambda)$ 的所有的根都看成复数时，这些根的实部都是负的（这也就是说，如果 $f(\lambda)$ 有实根，那么这些实根必须都是负的）。或者用几何的形象来说就是，如果把 $f(\lambda)$ 的所有的根都放在复平面中，它们都位于左半平面内。

这就提出了一个和多项式有关的代数学问题，即在什么条件下，实系数多项式

$$f(x) = a_0 + a_1x + \cdots + a_nx^n$$

的所有的根都具有负实部。

这一问题已为英国数学家劳思在1875年以及德国数学家胡尔维茨在1895年分别独立所解决。因此现在一般通称这一结果为劳思－胡尔维茨定理。下面我们就来介绍他们的结果。

劳思（Routh，Edward John，1831—1907），数学家．生于加拿大魁北克，座于英国剑桥．

胡尔维茨（Hurwitz，Adolf，1859—1919），德国数学家．生于希尔德斯海姆，卒于瑞士苏黎世．

虽然我们提出的问题是要解决实系数多项式的问题，但是为了解决这一问题和使得证明的论述简化统一，我们却要先绕一个弯，即先假设多项式的系数可以是复数，在这种最一般的情况下来研究问题。可能在研究的一开始，你会觉得这是多此一举，但是到后来就会发现证明时说起话来要比限于实系数的情况自由多了，也方便多了。

定义 11.1.1 设 $f(x) = a_0 + a_1x + \cdots + a_nx^n$ 是一个复系数多项式，如果 $f(x)$ 的所有根的实部都是负数，则称 $f(x)$ 是胡尔维茨多项式。

引理 11.1.1 设 α 是一个复数，$\mathrm{Re}\,\alpha \neq 0$，那么 α 和 $\frac{1}{\alpha}$ 的实部的符号相同。

证明 由 $\mathrm{Re}\,\alpha \neq 0$ 可知 $\alpha \neq 0$，因此 $\frac{1}{\alpha}$ 是有意义的。再由

$$\frac{1}{\alpha} = \frac{\bar{\alpha}}{\alpha\bar{\alpha}}, \alpha\bar{\alpha} > 0, \quad \mathrm{Re}\,\bar{\alpha} = \mathrm{Re}\,\alpha$$

即得引理。

定义 11.1.2 设 $f(x) = a_0 + a_1x + \cdots + a_nx^n$ 是一个复系数多项式，定义

$$f^*(x) = \bar{a}_0 + \bar{a}_1(-x) + \cdots + \bar{a}_n(-x)^n$$

显然有

引理 11.1.2

(1) $(f^*(x))^* = f(x)$；

(2) $(f(x)g(x))^* = f^*(x)g^*(x)$。

引理 11.1.3 设 $\mathrm{Re}\,\alpha < 0$，那么

当 $\mathrm{Re}\,z < 0$ 时，$0 \leqslant |z-\alpha| < |z+\bar{\alpha}|$；

当 $\mathrm{Re}\,z = 0$ 时，$0 < |z-\alpha| = |z+\bar{\alpha}|$；

当 $\mathrm{Re}\,z > 0$ 时，$0 \leqslant |z-\alpha| > |z+\bar{\alpha}|$。

证明 设 $z = u + vi$，$\alpha = a + bi$，则由引理的条件知 $a < 0$。由直接计算可知

$$|z+\bar{\alpha}|^2 - |z-\alpha|^2 = 4ua$$

由此即可得出引理中的不等式。其中当 $\mathrm{Re}\,z = 0$ 时，由于 $\mathrm{Re}\,\alpha < 0$，所以不可能出现 $|z-\alpha| = |z+\bar{\alpha}| = 0$ 的情况（否则将有 $z = \alpha = -\bar{\alpha}$，从而 $\mathrm{Re}\,\alpha = 0$，与

假设矛盾)。

引理 11.1.4 设 $f(x) = a_n(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$,那么

$$f^*(x) = (-1)^n\bar{a}_n(x+\bar{\alpha}_1)(x+\bar{\alpha}_2)\cdots(x+\bar{\alpha}_n)$$

证明 设 $\bar{f}(x) = \bar{a}_0 + \bar{a}_1x + \cdots + \bar{a}_nx^n$,那么由根与系数的关系可知

$$\alpha_1+\alpha_2+\cdots+\alpha_n = -\frac{a_{n-1}}{a_n}$$

$$\alpha_1\alpha_2+\alpha_1\alpha_3+\cdots+\alpha_{n-1}\alpha_n = \frac{a_{n-2}}{a_n}$$

$$\vdots$$

$$\alpha_1\alpha_2\cdots\alpha_n = (-1)^n\frac{a_0}{a_n}$$

在上面的各个式子两边取共轭就得到

$$\bar{\alpha}_1+\bar{\alpha}_2+\cdots+\bar{\alpha}_n = -\frac{\bar{a}_{n-1}}{\bar{a}_n}$$

$$\bar{\alpha}_1\bar{\alpha}_2+\bar{\alpha}_1\bar{\alpha}_3+\cdots+\bar{\alpha}_{n-1}\bar{\alpha}_n = \frac{\bar{a}_{n-2}}{\bar{a}_n}$$

$$\vdots$$

$$\bar{\alpha}_1\bar{\alpha}_2\cdots\bar{\alpha}_n = (-1)^n\frac{\bar{a}_0}{\bar{a}_n}$$

因而再次应用根与系数的关系就得到

$$\bar{f}(x) = \bar{a}_0+\bar{a}_1x+\cdots+\bar{a}_nx^n = \bar{a}_n(x-\bar{\alpha}_1)(x-\bar{\alpha}_2)\cdots(x-\bar{\alpha}_n)$$

因此

$$f^*(x) = \bar{f}(-x) = \bar{a}_n(-x-\bar{\alpha}_1)(-x-\bar{\alpha}_2)\cdots(-x-\bar{\alpha}_n) =$$
$$(-1)^n\bar{a}_n(x+\bar{\alpha}_1)(x+\bar{\alpha}_2)\cdots(x+\bar{\alpha}_n)$$

引理 11.1.5 设 $f(x)$ 是胡尔维茨多项式,那么

当 $\mathrm{Re}\, z < 0$ 时,$0 \leqslant |f(z)| < |f^*(z)|$;

当 $\mathrm{Re}\, z = 0$ 时,$0 < |f(z)| = |f^*(z)|$;

当 $\mathrm{Re}\, z > 0$ 时,$0 \leqslant |f(z)| > |f^*(z)|$。

证明 设 $\mathrm{Re}\, z < 0$,$f(x) = a_n(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$,其中 $\alpha_1, \alpha_2, \cdots, \alpha_n$ 是 $f(x)$ 的所有根,那么由引理的条件知

$$\mathrm{Re}\, \alpha_i < 0, \quad i = 1,2,\cdots,n$$

因此由引理 11.1.3 知

$$0 \leqslant |z-\alpha_i| < |z+\bar{\alpha}_i|, \quad i = 1,2,\cdots,n$$

因而由引理 11.1.4 即得

$$0 \leqslant |f(x)| = |a_n(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)| =$$
$$|a_n||x-\alpha_1||x-\alpha_2|\cdots|x-\alpha_n| <$$

$$|a_n||x+\bar{\alpha}_1||x+\bar{\alpha}_2|\cdots|x+\bar{\alpha}_n|=$$
$$|(-1)^n a_n(x+\bar{\alpha}_1)(x+\bar{\alpha}_2)\cdots(x+\bar{\alpha}_n)|=|f^*(x)|$$

其余两个不等式类似可得。

引理 11.1.6 设 α,β 是任意两个使得 $|\alpha|>|\beta|$ 的复数，那么 $f(x)$ 是胡尔维茨多项式的充分必要条件是 $g(x)=\alpha f(x)-\beta f^*(x)$ 是胡尔维茨多项式。

证明 必要性：设 $f(x)$ 是胡尔维茨多项式，并设 $x=z$ 是 $g(x)$ 的根。如果 $\operatorname{Re} z\geqslant 0$，那么由引理 11.1.5 可知 $|f(z)|\geqslant|f^*(z)|$，再由 $|\alpha|>|\beta|$ 就得出 $|\alpha f(z)|>|\beta f^*(z)|$。但是由于 $x=z$ 是 $g(x)$ 的根，因此又有 $|\alpha f(z)|=|\beta f^*(z)|$。这就得出矛盾。所得的矛盾说明如果 $x=z$ 是 $g(x)$ 的根，就必有 $\operatorname{Re} z<0$，也就是 $g(x)=\alpha f(x)-\beta f^*(x)$ 是胡尔维茨多项式。

充分性：反过来设 $g(x)=\alpha f(x)-\beta f^*(x)$ 是胡尔维茨多项式。那么由于 $|\alpha|>|\beta|$，所以首先 $\alpha^2-\beta^2\neq 0$，因而 $\lambda=\frac{\alpha}{\alpha^2-\beta^2}$，$\mu=-\frac{\beta}{\alpha^2-\beta^2}$ 是有意义的。仍由 $|\alpha|>|\beta|$ 就得出 $|\lambda|>|\mu|$，用 $|\lambda|>|\mu|$ 对 $g(x)=\alpha f(x)-\beta f^*(x)$ 应用必要性中已证明过的结论就得出 $\lambda g(x)-\mu^* g(x)$ 或者

$$\frac{\alpha}{\alpha^2-\beta^2}(\alpha f(x)-\beta f^*(x))-\left(-\frac{\beta}{\alpha^2-\beta^2}\right)(\alpha f(x)-\beta f^*(x))^*=$$
$$\frac{\alpha^2}{\alpha^2-\beta^2}f(x)-\frac{\alpha\beta}{\alpha^2-\beta^2}f^*(x)+\frac{\alpha\beta}{\alpha^2-\beta^2}f^*(x)-\frac{\beta^2}{\alpha^2-\beta^2}f(x)=f(x)$$

也是胡尔维茨多项式。这就证明了引理。

引理 11.1.7 设 $\operatorname{Re}\xi<0$，那么 $f(x)$ 是胡尔维茨多项式的充分必要条件是

(1) $|f(\xi)|<|f^*(\xi)|$；

(2) $F(x,\xi)=\dfrac{f^*(\xi)f(x)-f(\xi)f^*(x)}{x-\xi}$ 是胡尔维茨多项式。

证明 必要性：设 $f(x)$ 是胡尔维茨多项式。那么从 $\operatorname{Re}\xi<0$ 和引理11.1.5 就得出

$$|f(\xi)|<|f^*(\xi)| \quad 或 \quad |f^*(\xi)|>|f(\xi)|$$

因而由引理11.1.6又得出 $f^*(\xi)f(x)-f(\xi)f^*(x)$ 是胡尔维茨多项式。但是显然 $x=\xi$ 是此多项式的一个根。因而 $F(x,\xi)=\dfrac{f^*(\xi)f(x)-f(\xi)f^*(x)}{x-\xi}$ 是胡尔维茨多项式。(因为它的根的集合就是 $f^*(\xi)f(x)-f(\xi)f^*(x)$ 的所有的根的集合去掉 $x=\xi$ 这个根所得的集合)

充分性：反过来如果 $F(x,\xi)=\dfrac{f^*(\xi)f(x)-f(\xi)f^*(x)}{x-\xi}$ 是胡尔维茨多项式，那么因为 $\operatorname{Re}\xi<0$ 或 ξ 的实部为负就得知

$$(x-\xi)F(x,\xi)=f^*(\xi)f(x)-f(\xi)f^*(x)$$

是胡尔维茨多项式。再由 $|f^*(\xi)|>|f(\xi)|$ 和引理 11.1.6 就得出 $f(x)$ 是胡尔维茨多项式。

现在把 $F(x,\xi)$ 看成是一个二元多项式，则 $F(x,\xi)=F(\xi,x)$，且 $F(x,\xi)$ 关于 x 和 ξ 都是 $n-1$ 次的。因而可把 $F(x,\xi)$ 写成

$$F(x,\xi)=F_0(x)+F_1(x)\xi+\cdots+F_{n-1}(x)\xi^{n-1}$$

引理 11.1.8 设

$$H(x)=F_0(x)+\xi F_1(x)$$

$$\varphi(x)=\bar{a}_0x-\bar{a}_1\xi x+\bar{a}_0\xi,\quad \psi(x)=a_0x-a_1\xi x+a_0\xi$$

那么(1)
$$\bar{a}_0f(x)-a_0f^*(x)=xF_0(x)$$
$$-\bar{a}_1f(x)-a_1f^*(x)=-F_0(x)+xF_1(x)$$

(2)
$$x^2H(x)=f(x)\varphi(x)-f^*(x)\psi(x)$$

(3)$(\varphi^*(x)\varphi(x)-\psi^*(x)\psi(x))f(x)=x^2(H(x)\varphi^*(x)+H^*(x)\psi(x))$

证明 (1) 从 $F(x,\xi)$ 的定义可以得出

$$(x-\xi)F(x,\xi)=f^*(\xi)f(x)-f(\xi)f^*(x)$$

因此

$$(x-\xi)(F_0(x)+F_1(x)\xi+\cdots+F_{n-1}\xi^{n-1})=$$
$$f(x)(\bar{a}_0-\bar{a}_1\xi+\cdots+(-1)^n\bar{a}_n\xi^n)-f^*(x)(a_0+a_1\xi+\cdots+a_n\xi^n)$$

把上面的式子两边分别展开，然后比较 ξ 的同次幂的系数就可得出

$$\bar{a}_0f(x)-a_0f^*(x)=xF_0(x)$$
$$-\bar{a}_1f(x)-a_1f^*(x)=-F_0(x)+xF_1(x)$$

(2) 利用(1)，通过直接计算易于验证

$$x^2H(x)=x^2(F_0(x)+\xi F_1(x))=f(x)\varphi(x)-f^*(x)\psi(x)$$

(3) 由(2) 已证

$$x^2H(x)=f(x)\varphi(x)-f^*(x)\psi(x)$$

故由引理 11.1.2 得出

$$x^2H^*(x)=(x^2H(x))^*=(f(x)\varphi(x)-f^*(x)\psi(x))^*=$$
$$f^*(x)\varphi^*(x)-f(x)\psi^*(x)$$

用 $\varphi^*(x)$ 乘 $x^2H(x)$，用 $\varphi(x)$ 乘 $x^2H^*(x)$ 并把二式相加就得出

$$(\varphi^*(x)\varphi(x)-\psi^*(x)\psi(x))f(x)=x^2(H(x)\varphi^*(x)+H^*(x)\psi(x))$$

引理 11.1.9 设 $\mathrm{Re}\,\alpha>0,\mathrm{Re}\,\xi<0,\mathrm{Re}\left(\frac{a_1}{a_0}\right)>0$，那么 $|\varphi^*(\alpha)|>|\psi(\alpha)|$。

证明 当 $\mathrm{Re}\,b<0$时，一次多项式 $u(y)=y-b$ 显然是胡尔维茨多项式。因此由引理 1.11.4 知当 $\mathrm{Re}\,y<0$ 时成立

$$|u(\gamma)| < |u^*(\gamma)|$$

或者

$$|\gamma - b| < |-\gamma - \bar{b}|$$

令
$$b = \frac{1}{\xi}, \gamma = -\frac{a_1}{a_0} - \frac{1}{\alpha}$$

那么引理的条件保证 $\operatorname{Re} b < 0, \operatorname{Re} \gamma < 0$,因此可对上式所定义的 b 和 γ 应用不等式 $|\gamma - b| < |-\gamma - \bar{b}|$,这就得出

$$\left|\frac{a_1}{a_0} + \frac{1}{\alpha} + \frac{1}{\xi}\right| < \left|\frac{a_1}{a_0} + \frac{1}{\alpha} - \frac{1}{\bar{\xi}}\right|$$

由于 $|\xi| = |\bar{\xi}|$,故用 $|a_0\alpha\xi|$ 去乘上面的不等式的左边,用 $|a_0\alpha\bar{\xi}|$ 去乘上面的不等式的右边,就得出不等式

$$|a_1\alpha\xi + a_0\xi + a_0\alpha| < |a_1\alpha\bar{\xi} + a_0\bar{\xi} - a_0\alpha|$$

这就是

$$|\psi(\alpha)| < |\varphi^*(\alpha)| \quad 或 \quad |\varphi^*(\alpha)| < |\psi(\alpha)|$$

引理 11.1.10 设 $\operatorname{Re} \xi < 0, \operatorname{Re}\left(\frac{a_1}{a_0}\right) > 0$,那么 $H(x)$ 的次数是 $n - 1$。

证明 由引理 11.1.8 知

$$x^2 H(x) = f(x)\varphi(x) - f^*(x)\psi(x)$$

因此 $\deg H \leqslant n - 1$。如果 $\deg H < n - 1$,那么

$$\deg(f(x)\varphi(x) - f^*(x)\psi(x)) < n + 1$$

因此 $f(x)\varphi(x) - f^*(x)\psi(x)$ 中 x^{n+1} 的系数为 0。也就是

$$a_n(\bar{a}_0 - \bar{a}_1\xi) - (-1)^n\bar{a}_n(a_0 + a_1\xi) = 0$$

由此得出

$$|\bar{a}_0 - \bar{a}_1\xi| = |a_0 + a_1\xi|$$

或
$$\left|\frac{1}{\xi} - \frac{\bar{a}_1}{a_0}\right| = \left|\frac{1}{\xi} + \frac{a_1}{a_0}\right|$$

但是另一方面,当 $\operatorname{Re} c > 0$ 时,显然 $v(\gamma) = \gamma + c$ 是胡尔维茨多项式,因而由引理 1.11.5 知当 $\operatorname{Re} \gamma < 0$ 时

$$|v(\gamma)| < |v^*(\gamma)|$$

即
$$|\gamma + c| < |-\gamma + \bar{c}|$$

令 $c = \frac{a_1}{a_0}, \gamma = \frac{1}{\xi}$,那么引理的条件保证 $\operatorname{Re} c > 0, \operatorname{Re} \gamma < 0$,因此可对上式所定义的 c 和 γ 应用不等式 $|\gamma + c| < |-\gamma + \bar{c}|$,这就得出

$$\left|\frac{1}{\xi} + \frac{a_1}{a_0}\right| = \left|\frac{1}{\xi} - \frac{\bar{a}_1}{a_0}\right|$$

而这与 $\left|\frac{1}{\xi} - \frac{\bar{a}_1}{a_0}\right| = \left|\frac{1}{\xi} + \frac{a_1}{a_0}\right|$ 矛盾。所得的矛盾就说明不可能成立 $\deg H <$

$n-1$，由此即得出 $n-1 \leqslant \deg H \leqslant n-1$，因此 $\deg H = n-1$，即 $H(x)$ 的次数是 $n-1$。

引理 11.1.11 设 $\operatorname{Re}\xi < 0$，那么 $f(x)$ 是胡尔维茨多项式的充分必要条件是

(1) $a_0 \neq 0, \operatorname{Re}\left(\frac{a_1}{a_0}\right) > 0$；

(2) $n-1$ 次多项式 $H(x) = F_0(x) + \xi F_1(x)$ 是胡尔维茨多项式。

证明 必要性：设 $f(x)$ 是胡尔维茨多项式，那么由于 $f(x)$ 的所有的根的实部为负，所以 $f(x)$ 没有 0 根，因而 $a_0 \neq 0$。再由 $f(x)$ 的所有的根的实部为负和引理 11.1.1 可知 $f(x)$ 的所有的根的倒数的实部为负。故由根与系数的关系可知

$$\frac{1}{\alpha_1}+\frac{1}{\alpha_2}+\cdots+\frac{1}{\alpha_n} = \frac{\alpha_2\alpha_3\cdots\alpha_n+\alpha_1\alpha_3\cdots\alpha_n+\cdots+\alpha_1\alpha_2\cdots\alpha_{n-1}}{\alpha_1\alpha_2\cdots\alpha_n} = \frac{(-1)^{n-1}a_1}{(-1)^n a_0} = -\frac{a_1}{a_0}$$

由此就得出

$$\operatorname{Re}\left(\frac{a_1}{a_0}\right) = \operatorname{Re}\left(\frac{1}{\alpha_1}+\frac{1}{\alpha_2}+\cdots+\frac{1}{\alpha_n}\right) > 0$$

设 $\operatorname{Re}\sigma < 0$，$\alpha$ 是 $H(x) = F_0(x) + \xi F_1(x)$ 的根，那么由 $f(x)$ 是胡尔维茨多项式和引理 11.1.7 可知 $F(x,\sigma)$ 是胡尔维茨多项式。因此如果 $\operatorname{Re}\alpha \geqslant 0$，就必有 $F(\alpha,\sigma) \neq 0$ 因为否则 $F(x,\sigma)$ 就将有一个根不具有负实部，因而 $F(x,\sigma)$ 就不是胡尔维茨多项式了。

令 $\sigma = \frac{1}{\tau}$，那么由引理 11.1.1 可知 $\operatorname{Re}\tau < 0$。再令

$$\begin{aligned}\Phi(\alpha,\tau) &= \tau^{n-1}F\left(\alpha,\frac{1}{\tau}\right) = \tau^{n-1}\left(F_{n-1}(\alpha)\left(\frac{1}{\tau}\right)^{n-1} + F_{n-2}(\alpha)\left(\frac{1}{\tau}\right)^{n-2} + \cdots + F_0(\alpha)\right) = \\ &F_0(\alpha)\tau^{n-1} + F_1(\alpha)\tau^{n-2} + \cdots + F_{n-1}(\alpha)\end{aligned}$$

那么根据 Φ 的定义即可知 $\Phi(\alpha,\tau) \neq 0$。

以下分两种情况讨论：

(1) $F_0(\alpha) \neq 0$。这时 $\Phi(\alpha,\tau)$ 是 τ 的 $n-1$ 次多项式，其所有的根的实部非负（否则，如果 $\Phi(\alpha,\tau)$ 有一个根 z 使得 $\operatorname{Re} z < 0$，那么把 $\frac{1}{z}$ 看成 σ，用类似上面的论证就可证明 $\Phi(\alpha,\tau) = F\left(\alpha,\frac{1}{z}\right) \neq 0$，这与 z 是的 $\Phi(\alpha,\tau)$ 根矛盾）。设 $z_1, z_2, \cdots, z_{n-1}$ 是 $\Phi(\alpha,\tau)$ 的所有根，则由根与系数的关系可知

$$z_1 + z_2 + \cdots + z_n = -\frac{F_1}{F_0}$$

由此得出

$$\mathrm{Re}\left(-\frac{F_1}{F_0}\right) = \frac{1}{z_1} + \frac{1}{z_2} + \cdots + \frac{1}{z_{n-1}} \geqslant 0$$

但是另一方面，由于 α 是 $H(x)$ 的根，故

$$H(\alpha) = F_0(\alpha) + \xi F_1(\alpha) = 0$$

因此
$$\frac{1}{\xi} = -\frac{F_1(\alpha)}{F_0(\alpha)}$$

故
$$\mathrm{Re}\left(\frac{1}{\xi}\right) \geqslant 0$$

这与 $\mathrm{Re}\,\xi < 0$ 矛盾。

(2) $F_0(\alpha) = 0$。这时由 $H(\alpha) = F_0(\alpha) + \xi F_1(\alpha) = 0$ 得出 $F_1(\alpha) = 0$。因而由引理 11.1.8 得出

$$\bar{a}_0 f(\alpha) - a_0 f^*(\alpha) = 0, \quad \bar{a}_1 f(\alpha) + a_1 f^*(\alpha) = 0$$

因而

$$(\bar{a}_0 a_1 + a_0 \bar{a}_1) f(\alpha) = 0$$

由于 $\mathrm{Re}\,\alpha \geqslant 0$，而 $f(x)$ 是胡尔维茨多项式，因而 $f(\alpha) \neq 0$，$\bar{a}_0 a_1 + a_0 \bar{a}_1 = 0$，这也就是

$$\frac{a_1}{a_0} = -\frac{\bar{a}_1}{\bar{a}_0} = -\overline{\left(\frac{a_1}{a_0}\right)}$$

故 $\mathrm{Re}\left(\frac{a_1}{a_0}\right) = 0$，而这与已证的 $\mathrm{Re}\left(\frac{a_1}{a_0}\right) > 0$ 矛盾。

综合上面两种情况的讨论就说明如果 $\mathrm{Re}\,\alpha \geqslant 0$，则 α 不可能是 $H(x)$ 的根，因而 $H(x)$ 是胡尔维茨多项式。这就证明了必要性。

充分性：即设(1) $a_0 \neq 0$，$\mathrm{Re}\left(\frac{a_1}{a_0}\right) > 0$ 并且(2) $H(x)$ 是胡尔维茨多项式。

设 α 是 $f(x)$ 的根，如果 $\mathrm{Re}\,\alpha \geqslant 0$，那么由假设知 $H(x)$ 是胡尔维茨多项式。因此由引理 11.1.5 就得出

$$|H(\alpha)| > |H^*(\alpha)| \geqslant 0$$

由引理 11.1.9 知

$$|\varphi^*(\alpha)| > |\psi(\alpha)|$$

因此

$$|H(\alpha)\varphi^*(\alpha)| > |H^*(\alpha)\psi(\alpha)|$$

另一方面，由引理 11.1.8 知

$$(\varphi^*(x)\varphi(x) - \psi^*(x)\psi(x)) f(x) = x^2 (H(x)\varphi^*(x) + H^*(x)\psi(x))$$

由于 $a_n \neq 0$,所以 $\alpha \neq 0$。因而在上式中令 $x = \alpha$ 就得出

$$H(\alpha)\varphi^*(\alpha) + H^*(\alpha)\psi(\alpha) = 0$$

由此得出 $|H(\alpha)\varphi^*(\alpha)| = |H^*(\alpha)\psi(\alpha)|$ 与 $|H(\alpha)\varphi^*(\alpha)| > |H^*(\alpha)\psi(\alpha)|$ 矛盾。所得的矛盾就说明如果 $\mathrm{Re}\,\alpha \geqslant 0$,那么 α 就不可能是 $f(x)$ 的根,这也就是说 $f(x)$ 是胡尔维茨多项式。这就证明了充分性。

定理 11.1.1 劳思 - 胡尔维茨定理。

(1) 设 $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0$ 是一个实系数多项式,并且 $a_0 > 0$,那么 $f(x)$ 是胡尔维茨多项式,即 $f(x)$ 的所有根的都具有负实部的充分必要条件是以下的 n 个行列式都大于 0。

$$D_1 = a_1, D_2 = \begin{vmatrix} a_1 & a_0 \\ a_3 & a_2 \end{vmatrix}, D_3 = \begin{vmatrix} a_1 & a_0 & 0 \\ a_3 & a_2 & a_1 \\ a_5 & a_4 & a_3 \end{vmatrix}$$

$$D_4 = \begin{vmatrix} a_1 & a_0 & 0 & 0 \\ a_3 & a_2 & a_1 & a_0 \\ a_5 & a_4 & a_3 & a_2 \\ a_7 & a_6 & a_5 & a_4 \end{vmatrix}, \cdots, D_n = \begin{vmatrix} a_1 & a_n & 0 & \cdots & 0 \\ a_3 & a_{n-2} & a_1 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ a_{2n-1} & a_{2n-2} & a_{2n-3} & \cdots & a_n \end{vmatrix}$$

其中当 $i > n$ 时,$a_i = 0$。

(2) 设 $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$ 是一个实系数多项式,并且 $a_0 > 0$,那么 $f(x)$ 是胡尔维茨多项式,即 $f(x)$ 的所有根都具有负实部的充分必要条件是以下的 n 个行列式都大于 0。

$$D_1 = a_1, D_2 = \begin{vmatrix} a_1 & a_0 \\ a_3 & a_2 \end{vmatrix}, D_3 = \begin{vmatrix} a_1 & a_0 & 0 \\ a_3 & a_2 & a_1 \\ a_5 & a_4 & a_3 \end{vmatrix}$$

$$D_4 = \begin{vmatrix} a_1 & a_0 & 0 & 0 \\ a_3 & a_2 & a_1 & a_0 \\ a_5 & a_4 & a_3 & a_2 \\ a_7 & a_6 & a_5 & a_4 \end{vmatrix}, \cdots, D_n = \begin{vmatrix} a_1 & a_n & 0 & \cdots & 0 \\ a_3 & a_{n-2} & a_1 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ a_{2n-1} & a_{2n-2} & a_{2n-3} & \cdots & a_n \end{vmatrix}$$

其中当 $i > n$ 时,$a_i = 0$。

证明 设

$$g(x) = a_0 + a_2x^2 + a_2x^4 + \cdots, h(x) = a_1x + a_3x^3 + a_5x^5 + \cdots$$

那么显然

$$f(x) = g(x) + h(x), f^*(x) = g(x) - h(x)$$

把上式代入引理 11.1.8 中的

$$x^2H(x) = f(x)\varphi(x) - f^*(x)\psi(x)$$

就得到

$$x^2H(x)=2(a_0x+a_0\xi)h(x)-2a_1\xi xg(x)$$

令 $K(x)=\frac{1}{2}H(x)$，那么从上式就得到

$$K(x)=(a_0x+a_0\xi)h(x)-a_1\xi xg(x)=$$
$$a_0a_1-(a_1a_2-a_0a_3)\xi x+a_0a_3x^2-(a_1a_4-a_0a_5)\xi x^3+$$
$$a_0a_5x^4-(a_1a_6-a_0a_7)\xi x^5+\cdots$$

根据引理11.1.11知如果 $\operatorname{Re}\xi<0$，那么 $f(x)$ 是胡尔维茨多项式的充分必要条件是 $a_0>0,\operatorname{Re}\left(\frac{a_1}{a_0}\right)>0$ 并且 $H(x)$ 是胡尔维茨多项式。在 $f(x)$ 的系数是实系数的条件下，这一引理就相当于如果 $\operatorname{Re}\xi<0$，那么 $f(x)$ 是胡尔维茨多项式的充分必要条件是 $a_0>0,a_1>0$ 并且 $K(x)$ 是胡尔维茨多项式。

现在令 $\xi=-1$，那么显然 $\operatorname{Re}\xi<0$。这时

$$K(x)=a_0a_1+(a_1a_2-a_0a_3)x+a_0a_3x^2+(a_1a_4-a_0a_5)x^3+$$
$$a_0a_5x^4+(a_1a_6-a_0a_7)x^5+\cdots$$

而定理中的 n 个行列式对于 $K(x)$ 来说就成为

$$\Delta_1=a_1a_2-a_0a_3,\Delta_2=\begin{vmatrix}a_1a_2-a_0a_3 & a_0a_1\\ a_1a_4-a_0a_5 & a_0a_3\end{vmatrix},\cdots$$

$$\Delta_{n-1}=\begin{vmatrix}a_1a_2-a_0a_3 & a_0a_1 & 0 & \cdots & 0\\ a_1a_4-a_0a_5 & a_0a_3 & a_1a_2-a_0a_3 & \cdots & 0\\ \cdots & \cdots & \cdots & & \\ \cdots & \cdots & \cdots & & \end{vmatrix}$$

设 $\boldsymbol{M}_i$ 是与行列式 Δ_i 相对应的矩阵，那么由行列式按一行或一列展开的法则易于验证

$$a_0a_1\Delta_i=\begin{vmatrix}a_0a_1 & 0 & \cdots & 0\\ a_0a_3 & & & \\ a_0a_5 & & \boldsymbol{M}_i & \\ \cdots & \cdots & \cdots & \end{vmatrix}$$

在上面的行列式中，把第一列加到第二列上，把第三列加到第四列上，…就得到

当 i 是奇数时

$$a_0a_1\Delta_i=(a_0a_1)^{\frac{i+1}{2}}D_{i+1}$$

当 i 是偶数时

$$a_0a_1\Delta_i=a_0(a_0a_1)^{\frac{i}{2}}D_{i+1}$$

因此当 $a_0>0, a_1>0$ 时，Δ_i 与 D_{i+1} 同号。

下面用数学归纳法证明定理的部分(1)。

必要性：即设 $f(x)$ 是胡尔维茨多项式。

当 $n=1$ 时，$f(x)=a_0+a_1x$，因此由 $a_0>0$ 显然就得出 $a_1=D_1>0$。因此必要性对 $n=1$ 时成立。

假设必要性对不大于 $n-1$ 的所有自然数成立，那么就由 $a_0>0$ 和引理 11.1.11 得出 $a_1>0$ 并且 $K(x)$ 是胡尔维茨多项式。于是根据归纳法假设就有

$$\Delta_1>0, \Delta_2>0, \cdots, \Delta_{n-1}>0$$

因而根据上面已证的关于 Δ_i 与 D_{i+1} 的同号关系就得出

$$D_1=a_1>0, D_2>0, \cdots, D_{n-1}>0, D_n>0$$

这就说明，必要性对自然数 n 也成立，因而由数学归纳法就证明了必要性。

充分性：反之，设

$$D_1=a_1>0, D_2>0, \cdots, D_{n-1}>0, D_n>0$$

当 $n=1$ 时，$f(x)=a_0+a_1x$，因此由 $a_0>0, a_1=D_1>0$，显然就得出 $f(x)$ 是胡尔维茨多项式。

假设对不大于 $n-1$ 的所有自然数充分性成立，那么由

$$D_1=a_1>0, D_2>0, \cdots, D_{n-1}>0, D_n>0$$

和上面已证的关于 Δ_i 与 D_{i+1} 的同号关系就得出

$$\Delta_1>0, \Delta_2>0, \cdots, \Delta_{n-1}>0$$

故由归纳法假设可知 $K(x)$ 因而是 $H(x)$ 胡尔维茨多项式。再由引理 11.1.11 就得出 $f(x)$ 是胡尔维茨多项式。

这就说明，充分性对自然数 n 也成立，因而由数学归纳法就证明了充分性。

易于验证 $g(x)=x^nf(\frac{1}{x})$ 的所有根恰是 $f(x)$ 的所有根的倒数。故由引理 11.1.1 可知 $f(x)$ 是胡尔维茨多项式的充分必要条件是 $g(x)$ 是胡尔维茨多项式。然而由计算可知如果

$$f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n$$

那么

$$g(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0$$

因此对 $g(x)$ 应用定理部分(1)已证的结论就得到定理的部分(2)。

下面再给出一个 $f(x)$ 是胡尔维茨多项式的必要条件，这一必要条件虽然极其简单，但从上面的定理却不能明显看出。

定理 11.1.2 设 $f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n$ 是实系数多项式，$a_0>0$，那么 $f(x)$ 是胡尔维茨多项式的必要条件是 $f(x)$ 的所有系数为正数。

证明 由实域中多项式的唯一分解定理知 $f(x)$ 可分解为

$$f(x) = a_0 p_1 p_2 \cdots p_r q_1 q_2 \cdots q_s$$

其中 $p_i, i = 1,2,\cdots,r$ 都是首项为 1 的一次多项式，$q_j, j = 1,2,\cdots,s$ 都是首项为 1 的判别式小于 0 的二次多项式。

容易验证 p_i, q_j 为胡尔维茨多项式的必要条件是它们的所有系数为正数，而显然系数为正数的多项式的乘积仍是系数为正数的多项式，这就得出 $f(x)$ 是胡尔维茨多项式的必要条件是 $f(x)$ 的所有系数为正数。

不过容易举出反例说明当 $n \geqslant 3$ 时，上述条件并不是充分的。

例 11.1.1 多项式 $f(x) = 2 + x + x^2 + x^3$ 不是胡尔维茨多项式，因为对于它来说 $D_2 = -1$。

11.2 和 Hopf 分支有关的代数判据

考虑带参数 ϵ 的 n 维动力系统

$$\frac{\mathrm{d}X}{\mathrm{d}t} = F(X), X \in R^n, \epsilon \in R^m$$

设此系统有一个稳定的二维中心流形 $C(\epsilon)$，并设当 $\epsilon = 0$ 时 X_0 是此系统的稳定或不稳定的焦点，即设 $f(X_0) = 0$。又设在 ϵ 领域中的某一和 $\epsilon = 0$ 相连通的区域 U 内，当 $\epsilon \neq 0$，ϵ 充分小时，$X_0(\epsilon)$ 的稳定性发生突然的改变，那么在常微分方程理论中已经证明了：在 U 内将产生一个振幅很小的周期解，这就是所谓的 Hopf 分支。Hopf 分支在数学物理中都是一个很重要的研究内容。

设 $\boldsymbol{A}$ 是此系统的线性部分的系数矩阵，即设 $\boldsymbol{A} = \left.\frac{\partial F}{\partial X}\right|_{X = X_0}$，而 $f(\lambda)$ 是 $\boldsymbol{A}$ 的特征多项式。那么上述系统发生 Hopf 分支的一个必要条件是首先必须是中心型的奇点。具体说就是当 $\epsilon = 0$ 时，$\boldsymbol{A}$ 的特征多项式 $f(\lambda)$ 必须要有一对纯虚根，而其余的特征值都有负实部。这就引出另一个代数问题，就是如何判断一个多项式是否具有上述性质的问题。冯贝叶在 1988 年解决了 $n = 3$ 和 $n = 4$ 时判别问题，陈文成，陈国良 1992 年给出了一般情况下的解答。下面就来介绍他们的结果。

显然这一问题和 11.1 中的问题有密切的联系。

设

$$f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n$$

$$Q(x) = a_0 x^n + a_2 x^{n-2} + \cdots$$

$$R(x) = a_{n-1} x^{n-1} + a_{n-3} x^{n-3} + \cdots$$

$$P(x) = (a_1 - a_0 x)R(x) + a_1 Q(x) = a_1 R(x) + (a_1 Q(x) - a_0 x R(x)) =$$

$$a_1^2x^{n-1}+(a_1a_2-a_0a_3)x^{n-2}+a_1a_3x^{n-3}+(a_1a_4-a_0a_5)x^{n-4}+$$
$$a_1a_5x^{n-5}+(a_1a_6-a_0a_7)x^{n-6}+a_1a_7x^{n-7}+\cdots+a_1a_n$$

引理 11.2.1 设 $f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n, a_0\neq 0$ 的胡尔维茨行列式为

$$D_1,D_2,\cdots,D_{n-1},D_n$$

$P(x)$ 的胡尔维茨行列式为

$$\Delta_1',\Delta_2',\cdots,\Delta'_{n-1}$$

那么
$$\Delta'_i=a_1^{i-1}D_{i+1}, i=1,2,\cdots,n-1$$

证明 根据 $P(x)$ 的表达式不难验证它的胡尔维茨行列式为

$$\Delta_1'=a_1a_2-a_0a_3,\Delta_2'=\begin{vmatrix}a_1a_2-a_0a_3 & a_1^2\\ a_1a_4-a_0a_5 & a_1a_3\end{vmatrix},\cdots$$

$$\Delta'_{n-1}=\begin{vmatrix}a_1a_2-a_0a_3 & a_1^2 & 0 & \cdots & 0\\ a_1a_4-a_0a_5 & a_1a_3 & a_1a_2-a_0a_3 & \cdots & 0\\ \vdots & \vdots & \vdots & & \vdots\\ \cdots & \cdots & \cdots & \cdots & \cdots\end{vmatrix}$$

设 M_i' 是与行列式 Δ_i' 相对应的矩阵，那么由行列式按一行或一列展开的法则易于验证

$$a_0a_1\Delta_i'=\left|\begin{array}{c:ccc}a_0a_1 & 0 & \cdots & 0\\ \hdashline a_0a_3 & & & \\ a_0a_5 & & M_i' & \\ \cdots & \cdots & \cdots & \end{array}\right|$$

在上面的行列式中，把第一列加到第二列上，把第三列乘以$\dfrac{a_0}{a_1}$加到第四列上 … 就得到

$$a_0a_1\Delta_1'=a_0a_1D_2,\quad a_0a_1\Delta_2'=a_0a_1^2D_3,\cdots$$
$$a_0a_1\Delta_i'=a_0a_1^iD_{i+1}, i=1,2,\cdots,n-1$$

由于 $a_0\neq 0$，故可在上述等式两边约去 a_0，这就证明了引理。

引理 11.2.2 设 $f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n, a_0\neq 0$ 是实系数多项式，那么 $f(\pm\omega\mathrm{i})=0$ 的充分必要条件是 $P(\pm\omega\mathrm{i})=0$。

证明 显然有

$$f(x)=Q(x)+R(x),(-1)^nf(-x)=Q(x)-R(x)$$

由此得出

$$Q(x)=\frac{1}{2}(f(x)+(-1)^nf(-x)),R(x)=\frac{1}{2}(f(x)-(-1)^nf(-x))$$

假设 $f(\omega i)=0$，由于 $f(x)$ 是实系数多项式，因此它的复数根和它的共轭复根是成对出现的，这就是说也有 $f(-\omega i)=0$，把 $f(\omega i)=0$ 和 $f(-\omega i)=0$ 代入上面的式子就得出 $Q(\omega i)=0, R(\omega i)=0$ 反过来，由 $Q(\omega i)=0, R(\omega i)=0$ 显然立刻得出 $f(\omega i)=0$，同理由 $f(-\omega i)=0$ 可以得出 $Q(-\omega i)=0$，$R(-\omega i)=0$ 反过来也是如此。

再由 $P(x)=(a_1-a_0x)R(x)+a_1Q(x)$ 和 $-P(-x)=(a_1+a_0x)R(x)-a_1Q(x)$ 同理可证 $P(\pm\omega i)=0$ 的充分必要条件是 $Q(\pm\omega i)=0$ 并且 $R(\pm\omega i)=0$。

这就证明了引理。

引理 11.2.3 设

$$f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n=$$
$$a_0(x^2+\omega^2)(x^{n-2}+b_1x^{n-3}+\cdots+b_{n-3}x+b_{n-2})$$

又设 $D_1, D_2, \cdots, D_{n-1}, D_n$ 为 $f(x)=x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n$ 的胡尔维茨行列式，$d_1, d_2, \cdots, d_{n-2}$ 为 $x^{n-2}+b_1x^{n-3}+\cdots+b_{n-3}x+b_{n-2}$ 的胡尔维茨行列式，则

(1)
$$a_1=a_0b_1$$
$$a_2=a_0(b_2+\omega^2)$$
$$a_i=a_0(b_i+\omega^2b_{i-2}),\quad i=3,4,\cdots,n-2$$
$$a_{n-1}=a_0\omega^2b_{n-3}$$
$$a_n=a_0\omega^2b_{n-2}$$

(2)
$$D_k=a_0^kd_k, k=1,2,,n-2, D_{n-1}=0$$

证明 (1) 把 $a_0(x^2+\omega^2)(x^{n-2}+b_1x^{n-3}+\cdots+b_{n-3}x+b_{n-2})$ 展开，合并同类项并与 $f(x)$ 比较同次幂的系数就得到(1) 中的式子。

(2)
$$D_1=a_1=a_0b_1=a_0d_1$$

$$D_2=\begin{vmatrix}a_1 & a_0\\ a_3 & a_2\end{vmatrix}=\begin{vmatrix}a_0b_1 & a_0\\ a_0(b_3+\omega^2b_1) & a_0(b_2+\omega^2)\end{vmatrix}=a_0^2\begin{vmatrix}b_1 & 1\\ b_3 & b_2\end{vmatrix}=a_0^2d_2$$

一般的，利用(1) 中的式子，依次将 D_k 的第1行乘以 $-\omega^2$ 加到第2行，再把第2行乘以 $-\omega^2$ 加到第3行，…，再把第 $n-3$ 行乘以 $-\omega^2$ 加到第 $n-2$ 行，就得到

$$D_k=a_0^kd_k, k=1,2,\cdots,n-2$$

最后再把第 $n-2$ 行乘以 $-\omega^2$ 加到第 $n-1$ 行，并注意当 $i>n-2$ 时，$b_i=0$ 就得到

$$D_{n-1} = a_0^{n-1}\begin{vmatrix} b_1 & 1 & 0 & \cdots & 0 \\ b_3 & b_2 & b_1 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ b_{2n-5} & b_{2n-6} & b_{2n-7} & \cdots & b_{n-3} \\ 0 & 0 & 0 & \cdots & 0 \end{vmatrix} = 0$$

引理 11.2.4 设 $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ 是实系数多项式，$a_0 > 0, a_1 > 0, a_n \neq 0$，那么 $f(x)$ 有一对纯虚根 $\pm \omega i$，且其余 $n-2$ 个根均具有负实部的充分必要条件是 $P(x)$ 有一对纯虚根 $\pm\omega i$，且其余 $n-3$ 个根均具有负实部。

证明 必要性：设 $f(x)$ 有一对纯虚根 $\pm\omega i$，且其余 $n-2$ 个根均具有负实部，则由引理 11.2.2 知 $P(x)$ 也有一对纯虚根 $\pm\omega i$，因此可将 $f(x)$，$P(x)$ 分别写成

$$f(x) = a_0(x^2+\omega^2)(x^{n-2} + b_1x^{n-3} + \cdots + b_{n-2})$$
$$P(x) = a_1^2(x^2+\omega^2)(x^{n-3} + b_1'x^{n-4} + \cdots + b'_{n-3})$$

由引理 11.2.1 知若设 $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n, a_0 \neq 0$ 的胡尔维茨行列式为 $D_1, D_2, \cdots, D_{n-1}, D_n$，$P(x)$ 的胡尔维茨行列式为 Δ_1'，$\Delta_2', \cdots, \Delta'_{n-1}$。那么

$$\Delta_i' = a_1^{i-1}D_{i+1}, \quad i = 1,2,\cdots,n-1$$

又设 $\delta_k', d_k, k = 1,2,\cdots,n-3$ 分别是多项式

$$x^{n-3} + b_1'x^{n-4} + \cdots + b'_{n-3}$$

和多项式

$$x^{n-2} + b_1x^{n-3} + \cdots + b_{n-2}$$

的胡尔维茨行列式。那么由引理 11.2.3 中的 $D_k = a_0^k d_k, k = 1,2,\cdots,n-2$ 和上面的 $\Delta_i' = a_1^{i-1}D_{i+1},\quad i = 1,2,\cdots,n-1$ 就得到

$$\delta_k' = \frac{\Delta_k'}{(a_1^2)^k} = \frac{a_1^kD_{k+1}}{a_1^{2k}} = \frac{a_0^{k+1}}{a_1^{k+1}}d_{k+1}, \quad k = 1,2,\cdots,k+3$$

由于 $x^{n-2} + b_1x^{n-3} + \cdots + b_{n-2}$ 的根都具有负实部，因此由胡尔维茨定理知 d_1，$d_2, \cdots, d_{n-2}$ 都是正的，因而 $\delta_1', \delta_2', \cdots, \delta'_{n-3}$ 都是正的，这就说明 $P(x)$ 有一对纯虚根 $\pm\omega i$，且其余 $n-3$ 个根均具有负实部。

充分性：反过来假设 $P(x)$ 有一对纯虚根 $\pm\omega i$，且其余 $n-3$ 个根均具有负实部。那么根据上面已证明的结论可知 $f(x)$ 也有一对纯虚根 $\pm\omega i$，且 δ_1'，$\delta_2', \cdots, \delta'_{n-3}$ 都是正的，因而 $d_2, \cdots, d_{n-2}$ 都是正的，又 $d_1 = b_1 = \dfrac{a_1}{a_0} > 0$，所以 $f(x)$ 有一对纯虚根 $\pm\omega i$，且其余 $n-2$ 个根均具有负实部。

综合上面两部分的论述就证明了引理。

定理 11.2.1 设 $f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n$ 是实系数多项式，$a_0>0,a_n\neq 0$。又设 $f(x)$ 的胡尔维茨行列式为 $D_1,D_2,\cdots,D_{n-1},D_n$，那么

(1)$f(x)$ 有一对纯虚根 $\pm\omega\mathrm{i}$，且其余 $n-2$ 个根均具有负实部的充分必要条件是并且

$$D_{n-1}=0$$

并且

$$D_1>0,D_2>0,\cdots,D_{n-2}>0,a_n>0$$

(2) $$\omega^2=\frac{D_{n-3}}{D_{n-2}}a_n\quad（我们规定 D_{-1}=\frac{1}{a_0},D_0=1）$$

证明 (1) 必要性：设 $f(x)$ 有一对纯虚根 $\pm\omega\mathrm{i}$，且其余 $n-2$ 个根均具有负实部。那么

$$f(x)=a_0(x^2+\omega^2)(x^{n-2}+b_1x^{n-3}+\cdots+b_{n-2})$$

其中多项式 $x^{n-2}+b_1x^{n-3}+\cdots+b_{n-2}$ 的根均具有负实部。于是若设它的胡尔维茨行列式为 $d_1,d_2,\cdots,d_{n-2}$ 的话，根据胡尔维茨定理就可知 $d_k>0,k=1,2,\cdots,n$。由这些不等式和引理 11.2.3 得出 $D_k>0,k=1,2,\cdots,n-2,D_{n-1}=0$。又由定理 11.1.2 知当 $a_0>0$ 时胡尔维茨多项式的系数都是整数，因此 $b_1>0,b_2>0,\cdots,b_{n-2}>0$，由此和引理 11.2.3 就得出 $a_n>0$。这就证明了必要性。

充分性：即设 $a_0>0,D_k>0,k=1,2,\cdots,n-2,D_{n-1}=0,a_n>0$。

我们用数学归纳法证明。

当 $n=2$ 时，$f(x)=a_0x^2+a_1x+a_2$。上述条件就是 $a_0>0,D_1=a_1=0,a_2>0$。显然在此条件下，$f(x)$ 显然有一对纯虚根。

当 $n=2$ 时，$f(x)=a_0x^2+a_1x^2+a_2x+a_3$。上述条件成为

$$a_0>0,D_1=a_1=0,D_2=\begin{vmatrix}a_1 & a_0\\ a_3 & a_2\end{vmatrix}=0$$

或 $$a_2=\frac{a_0a_3}{a_1},\quad a_3>0$$

在此条件下易于验证

$$f(x)=a_0\left(x^2+\frac{a_3}{a_1}\right)\left(x+\frac{a_1}{a_0}\right)$$

显然 $f(x)$ 有一对纯虚根和一个负根。因此充分性对于 $n=2$ 和 $n=3$ 的情况都成立。

假设充分性对于自然数 $n-1$ 的情况成立。则设 $P(x)$ 的胡尔维茨行列式为 $\boldsymbol{\Delta}_1',\boldsymbol{\Delta}_2',\cdots,\boldsymbol{\Delta}'_{n-1}$，那么由充分性条件和引理 11.2.1 可知

$$\boldsymbol{\Delta}_1'>0,\boldsymbol{\Delta}_2'>0,\cdots,\boldsymbol{\Delta}'_{n-3}>0,\boldsymbol{\Delta}'_{n-2}=0,a_1a_n>0$$

于是由归纳法假设得知 $P(x)$ 有一对纯虚根 $\pm\omega\mathrm{i}$，而其余的 $n-3$ 个根均具有

负实部。因而再由引理11.2.4就得出$f(x)$有一对纯虚根$\pm\omega i$,而其余的$n-2$个根均具有负实部。这就证明了充分性对于自然数n的情况也成立。因而由数学归纳法就证明了充分性。

现在我们已经知道,如果$a_0>0, D_k>0, k=1,2,\cdots,n-2, D_{n-1}=0, a_n>0$,那么$f(x)$必有一对纯虚根$\pm\omega i$,而其余的$n-2$个根均具有负实部。现在我们要问,这个$\omega$是否能用$f(x)$的系数明显地表示出来?答案是肯定的。

(2) 我们用数学归纳法证明。

当$n=2$时

$$D_1=a_1=0, f(x)=a_0x^2+a_2, \omega^2=\frac{a_2}{a_0}=\frac{D_{-1}}{D_0}a_2$$

当$n=3$时

$$D_2=\begin{vmatrix} a_1 & a_0 \\ a_3 & a_2 \end{vmatrix}=0$$

因此$a_2=\dfrac{a_0a_3}{a_1}$。这时

$$f(x)=a_0x^3+a_1x^2+a_2x+a_3=a_0\left(x^2+\frac{a_3}{a_1}\right)(x+a_1)$$

而

$$\omega^2=\frac{a_3}{a_1}=\frac{D_0}{D_1}a_3$$

当$n=4$时,$D_3=0$,因此$a_2=\dfrac{a_1^2a_4+a_0a_3^2}{a_1a_3}$,这时

$$f(x)=a_0x^4+a_1x^3+a_2x^2+a_3x+a_4=a_0\left(x^2+\frac{a_3}{a_1}\right)\left(x^2+\frac{a_1}{a_0}x+\frac{a_1a_4}{a_0a_3}\right)$$

而

$$\frac{D_1}{D_2}a_4=\frac{a_1a_4}{a_1a_2-a_0a_3}=\frac{a_1}{a_3}$$

因此

$$\omega^2=\frac{a_1}{a_3}=\frac{D_1}{D_2}a_4$$

以上的例子表明定理11.2.1的第(2)部分对于$n=2,3,4$的情况都是成立的。

现在设定理11.2.1的第(2)部分对于所有小于n的自然数都成立。那么根据定理的条件可知$f(x)$有一对纯虚根$\pm\omega i$,而其余的$n-2$个根都具有负实部。于是由引理11.2.4可知$P(x)$有一对纯虚根$\pm\omega i$,而其余的$n-3$个根都具有负实部。注意$P(x)$的首项系数是a_1^2,常数项是a_1a_n。因此根据归纳法假设就有

$$\omega^2=\frac{\Delta'_{n-4}}{\Delta'_{n-3}}a_1a_n$$

其中 $\Delta_1', \Delta_2', \cdots, \Delta'_{n-1}$ 是 $P(x)$ 的胡尔维茨行列式，再由引理 11.2.1 中的公式

$$\Delta_i' = a_1^{i-1} D_{i+1}, \quad i = 1,2,\cdots,n-1$$

就得出

$$\omega^2 = \frac{\Delta'_{n-4}}{\Delta'_{n-3}} a_1 a_n = \frac{D_{n-3}}{D_{n-2}} a_n$$

这就说明定理 11.2.1 的第(2)部分对于自然数 n 仍然成立。故由数学归纳法，我们就证明了(2)。

习题 11.2

1. 设 $f(x) = a_0x^4 + a_1x^3 + a_2x^2 + a_3x + a_4$，证明：当

$$a_0 > 0, a_1 > 0, a_2 = \frac{a_1^2 a_4 + a_0 a_3^2}{a_1 a_3} > 0, a_3 > 0, a_4 > 0$$

时，$f(x)$ 有一对纯虚根，并且其余的两个根均具有负实部。

2. 设 $f(x) = a_0x^5 + a_1x^4 + a_2x^3 + a_3x^2 + a_4x + a_5, a_0 > 0, D_1, D_2, \cdots, D_4, D_5$ 是 $f(x)$ 的胡尔维茨行列式。又设 $\bar{f}(x) = a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0, a_5 > 0, \bar{D}_1, \bar{D}_2, \cdots, \bar{D}_4, \bar{D}_5$ 是 $\bar{f}(x)$ 的胡尔维茨行列式。具体算出 $D_1, D_2, \cdots, D_4, D_5$ 和 $\bar{D}_1, \bar{D}_2, \cdots, \bar{D}_4, \bar{D}_5$ 的表达式来，并证明：$\bar{D}_4 = D_4, D_5 = a_5 D_4$。

3. 设 $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n, a_0 > 0, D_1, D_2, \cdots, D_{n-1}, D_n$ 是 $f(x)$ 的胡尔维茨行列式。$\bar{f}(x) = a_0 + a_1x + \cdots + a_nx^n, a_0 > 0, \bar{D}_1, \bar{D}_2, \cdots, \bar{D}_{n-1}, \bar{D}_n$ 是 $\bar{f}(x)$ 的胡尔维茨行列式。证明：

(1) $D_n = a_n D_{n-1}, \bar{D}_n = a_0 \bar{D}_{n-1}$；

(2) $\bar{D}_{n-1} = D_{n-1}$。

4. 设 $f(x) = 2x^4 + x^3 + 5x^2 + x + 3$。

(1) 计算：$K(x) = a_0a_1 + (a_1a_2 - a_0a_3)x + a_0a_3x^2 + (a_1a_4 - a_0a_5)x^3 + \cdots$；

(2) 设 $Q(x) = a_0x^n + a_2x^{n-2} + \cdots, R(x) = a_1x^{n-1} + a_3x^{n-3} + \cdots$，计算：$P(x) = (a_1 - a_0x)R(x) + a_1Q(x)$；

(3) 设对于 $K(x)$ 而言的 $K(x)$ 为 $K_1(x)$（也就是把 $K(x)$ 看成 $f(x)$ 时的 $K(x)$）。对于 $P(x)$ 而言的 $P(x)$ 为 $P_1(x)$（也就是把 $P(x)$ 看成 $f(x)$ 时的 $P(x)$）。计算 $K_1(x)$ 与 $P_1(x)$。

11.3 插值多项式和最小二乘法

多项式是一种特别简单的函数，而且有着很好的性质。而有的函数又很复杂，因此数学家很早就考虑过是否能用多项式去逼近任意的连续函数的问题。

假设你现在想用一个多项式 $P(x)$ 去逼近一个任意的连续函数 $f(x)$。最好的逼近结果当然就是干脆对所有的自变量的值 x 都有 $P(x) = f(x)$。不过这样一来，你那个原来假设的任意连续函数就不能是任意的了，它自己已经是一个多项式了。所以一般来说这是不可能的。因此我们只好后退一下，考虑只在有限的一些点 $x_1, x_2, \cdots, x_n$，让 $P(x_i) = f(x_i) = y_i, i = 1,2,\cdots,n$。这就引出以下的问题：

已知函数 $y = f(x)$ 在 $n+1$ 个点 $x_1, x_2, \cdots, x_n, x_{n+1}$ 上的值为 $y_1, y_2, \cdots, y_n, y_{n+1}$，要求一个次数不高于 n 的多项式 $L_n(x)$，使得 $L_n(x_i) = y_i, i = 1,2,\cdots,n, n+1$。

这个问题如果你不是这么抽象地提，而是搞得具体些，例如求多项式 $f(x) = ax^2 + bx + c$，使得 $f(1) = 1, f(2) = 2, f(3) = 3$ 之类，就是一般的中学生也会做。做法大体上是从条件得出

$$a + b + c = 1$$
$$4a + 2b + 2 = 2$$
$$9a + 3b + c = 3$$

然后去解上面的方程组，解出来之后，问题就解决了。不过如果企图用这种办法去解决上面的一般性的问题就会产生一些麻烦，一个是当 n 比较大时，这个解方程组的计算就是很繁琐的。如果每次都这么搞，也是够令人头疼的。即使你不怕繁琐的计算，那你总得担心是否会算了半天，最后要是无解怎么办的问题吧！这个是不是有解也不是一眼就能看出来的。所以就要另想办法。

法国数学家拉格朗日就想到了一个很巧妙的方法。其实这个方法的原理真是十分简单，就像搭积木一样。

任意取一个点 x_i。拉格朗日的想法是求一个多项式 $l_i(x)$，使得 $l_i(x_i) = 1$，而在其他的点处都等于 0。

这个想法的好处在哪呢？首先这里的 $l_i(x)$ 根本与 y_i 无关，所以适应性极广，而且可以预先构造，一旦对一批点 $x_1, x_2, \cdots, x_n, x_{n+1}$ 构造好了，对任意的 $y_i, i = 1,2,\cdots,n,n+1$ 都可以用；其次这里的 $l_i(x)$ 对所有的点造法都是一样的。最后显然可以看出，一旦构造出来了这些 $l_i(x)$，那么就有

$$L_n(x) = y_1 l_1(x) + y_2 l_2(x) + \cdots + y_n l_n(x) + y_{n+1} l_{n+1}(x)$$

所以不存在什么有解没解的问题，上面的式子就告诉你，肯定有解。

现在我们就来考虑如何求出 $l_i(x)$ 的问题。这也特别简单，因为既然除了 x_i 外，$l_i(x)$ 在其他的点处都等于 0，那就相当于说

$$l_i(x) = a_i(x - x_1)(x - x_2)\cdots(x - x_{i-1})(x - x_{i+1})\cdots(x - x_n)$$

所以原先那些什么计算繁琐，有没有解之类的问题全都不需考虑了，只剩下一个求系数 a_i 的问题了。这个问题也很好解决，只要用条件 $l_i(x_i) = 1$ 就立刻可

以求出

$$a_i = \frac{1}{(x_i - x_1)(x_i - x_2)\cdots(x_i - x_{i-1})(x_i - x_{i+1})\cdots(x_i - x_n)}$$

于是

$$L_n(x) = \sum_{k=1}^{n+1} \frac{(x - x_1)(x - x_2)\cdots(x - x_{k-1})(x - x_{k+1})\cdots(x - x_n)}{(x_k - x_1)(x_k - x_2)\cdots(x_k - x_{k-1})(x_k - x_{k+1})\cdots(x_k - x_n)} y_k$$

由于和号中的每个多项式都是 n 次的，所以 $L_n(x)$ 的次数不高于 n。

这一公式的唯一缺点就是没有把 $L_n(x)$ 直接表示出来。不过我觉得即使是用这种方法先把 $L_n(x)$ 写出来，再通过展开合并最后得出 $L_n(x)$ 的明显表达式也比用待定系数法去解方程组好受一些，起码在运算时可以节省不少纸面。例如用这一方法去求上面所提的求一个二次多项式 $f(x)$，使得 $f(1) = 1, f(2) = 2, f(3) = 3$ 的问题就有

$$f(x) = 1 \cdot \frac{(x-2)(x-3)}{(1-2)(1-3)} + 2 \cdot \frac{(x-1)(x-3)}{(2-1)(2-3)} + 3 \cdot \frac{(x-1)(x-2)}{(3-1)(3-2)} =$$

$$\frac{1}{2}(x^2 - 5x + 6) - 2(x^2 - 4x + 3) + \frac{3}{2}(x^2 - 3x + 2) =$$

$$\frac{1}{2}x^2 - \frac{5}{2}x + 3 - 2x^2 + 8x - 6 + \frac{3}{2}x^2 - \frac{9}{2}x + 3 = x$$

哈哈，看到这，你是不是又觉得连上面那么算都是多余的，这本来就是一眼就能看出来的。不过这已是马后炮了。从马后炮的观点看，什么事情都不能算难的。不过，刚开始时，放几下马后炮倒也没有什么坏处，起码说明你还是想了一下，在自己心里多放几次马后炮，经验多了，可能有一次你也可以放“马前炮”了。

所以现在我们已经有了一个解决插值问题的公式了，这一公式称为拉格朗日公式。不过这个公式毕竟还有点庞大，我们现在想法把它写得更紧凑些。设

$$l(x) = (x - x_1)(x - x_2)\cdots(x - x_n)(x - x_{n+1})$$

那么

$$\ln l(x) = \sum_{k=1}^{n+1} \ln(x - x_k)$$

在上式两边求导数就得到

$$\frac{l'(x)}{l(x)} = \sum_{k=1}^{n+1} \frac{1}{x - x_k}$$

$$l'(x) = \sum_{k=1}^{n+1} \frac{l(x)}{x - x_k} = \sum_{k=1}^{n+1} (x - x_1)(x - x_2)\cdots(x - x_{k-1})(x - x_{k+1})\cdots(x - x_n)$$

$$l'(x_k) = (x_k - x_1)(x_k - x_2)\cdots(x_k - x_{k-1})(x_k - x_{k+1})\cdots(x_k - x_n)$$

因而

$$L_n(x) = \sum_{k=1}^{n+1} \frac{l(x)}{(x - x_k)l'(x_k)} y_k$$

用这个公式去求上面例子中的多项式，做法就是先求出

$$l(x)=(x-1)(x-2)(x-3)=x^3-6x^2+11x-6$$

然后求出 $$l'(x)=3x^2-12x+11$$

因而有 $$l'(1)=2, l'(2)=-1, l'(3)=2$$

因此最后就有

$$f(x)=L_3(x)=\frac{1}{2}(x-2)(x-3)-2\cdot\frac{1}{2}(x-1)(x-3)+$$

$$3\frac{1}{2}(x-1)(x-2)=x$$

根据上面的讨论我们就有

定理 11.3.1 设给定了两两不同的 $n+1$ 个点 $x_1,x_2,\cdots,x_n,x_{n+1}$ 以及 $n+1$ 个值 $y_1,y_2,\cdots,y_n,y_{n+1}$，那么

(1) 存在唯一的一个次数不高于 n 的多项式 $L_n(x)$ 使得

$$L_n(x_i)=y_i, i=1,2,\cdots,n,n+1$$

(2) $L_n(x)=\sum\limits_{k=1}^{n+1}\frac{l(x)}{(x-x_k)l'(x_k)}y_k$，其中

$$l(x)=(x-x_1)(x-x_2)\cdots(x-x_n)(x-x_{n+1})$$

证明 存在性在上面的讨论中已经给出，所以只须证明唯一性即可。设还存在一个次数不高于 n 的多项式 $\bar{L}_n(x)$，使得 $\bar{L}_n(x)=y_i, i=1,2,\cdots,n,n+1$；由于 $L_n(x)$ 与 $\bar{L}_n(x)$ 都是次数不高于 n 的多项式，而它们在 $n+1$ 个两两不相同的点处取相同的值，因此由定理 10.1.4 即得 $L_n(x)=\bar{L}_n(x)$。这就证明了唯一性。

虽然上面的定理已经完全解决了插值多项式的存在性和唯一性问题。然而在使用中这一公式还是有一个不方便之处。问题在于当我们想用一个多项式去逼近一个函数时，我们总是想用最简单的多项式来达到目的，所谓最简单也就是次数尽可能的低。然而这往往是一件摸着石头过河的事，也就是说，你得试验着来。因此就存在着一种可能性，即第一次你取了比如说 n 个点，结果却发现不满意，于是你想再增加一个点去逼近。这时你就会发现，用上面的公式去做时，第二次要全部重算，而你辛辛苦苦算出来的第一次数据将全部作废。于是我们想问，如果第二次插值时，有 n 个点与第一次完全相同，是不是能有一个公式，可以将第一次所算出来的结果都用上，让我们节省一点劳动力。答案是肯定的。这就是用差分的理论得出的公式，而差分理论本身也有许多有趣的地方。

定义 11.3.1 设 $f(x)$ 是 x 的函数，那么

(1) $f(x_1,x_2)=\frac{f(x_2)-f(x_1)}{x_2-x_1}$ 称为 $f(x)$ 的一阶均差或差商；

(2) $f(x_1,x_2,x_3)=\frac{f(x_2,x_3)-f(x_1,x_2)}{x_3-x_1}$ 称为 $f(x)$ 的二阶均差或差商；一

般的,假设已经定义 $f(x)$ 的 $n-1$ 阶均差或差商 $f(x_1,x_2,\cdots,x_n)$;那么

(3) $f(x_1,x_2,\cdots,x_n,x_{n+1}) = \dfrac{f(x_2,x_3,\cdots,x_{n+1})-f(x_1,x_2,\cdots,x_n)}{x_{n+1}-x_1}$ 称为 $f(x)$ 的 n 阶均差或差商。

引理 11.3.1

$$f(x_1,x_2,\cdots,x_n)=\frac{f(x_1)}{(x_1-x_2)\cdots(x_1-x_n)}+\frac{f(x_2)}{(x_2-x_1)\cdots(x_2-x_n)}+\cdots+\frac{f(x_n)}{(x_n-x_1)\cdots(x_n-x_{n-1})}$$

因而均差或差商与分点的次序无关。

证明 当 $n=2$ 时

$$f(x_1,x_2)=\frac{f(x_2)-f(x_1)}{x_2-x_1}=\frac{f(x_1)}{x_1-x_2}+\frac{f(x_2)}{x_2-x_1}$$

当 $n=3$ 时

$$f(x_1,x_2,x_3)=\frac{f(x_2,x_3)-f(x_1,x_2)}{x_3-x_1}=\frac{f(x_1)}{(x_1-x_2)(x_1-x_3)}+\frac{f(x_2)}{(x_2-x_1)(x_2-x_3)}+\frac{f(x_3)}{(x_3-x_1)(x_3-x_2)}$$

因此对自然数 $n=2$ 和 $n=3$ 引理成立。

假设对自然数 $n-1$ 引理成立,那么

$$f(x_1,x_2,\cdots,x_n,x_{n+1})=\frac{f(x_2,x_3,\cdots,x_{n+1})-f(x_1,x_2,\cdots,x_n)}{x_{n+1}-x_1}=$$

$$\frac{1}{x_{n+1}-x_1}\left(\frac{f(x_2)}{(x_2-x_3)\cdots(x_2-x_{n+1})}+\frac{f(x_3)}{(x_3-x_1)\cdots(x_3-x_{n+1})}+\cdots+\frac{f(x_{n+1})}{(x_{n+1}-x_1)\cdots(x_{n+1}-x_n)}\right)-\frac{1}{x_{n+1}-x_1}\left(\frac{f(x_1)}{(x_1-x_2)\cdots(x_1-x_n)}+\frac{f(x_2)}{(x_2-x_1)\cdots(x_2-x_n)}+\cdots+\frac{f(x_n)}{(x_n-x_1)\cdots(x_n-x_n)}\right)=$$

$$\frac{f(x_1)}{(x_1-x_2)\cdots(x_1-x_{n+1})}+$$

$$\frac{f(x_2)}{x_{n+1}-x_1}\left(\frac{1}{(x_2-x_3)\cdots(x_2-x_{n+1})}-\frac{1}{(x_2-x_1)\cdots(x_2-x_n)}\right)+\cdots+$$

$$\frac{f(x_n)}{x_{n+1}-x_1}\left(\frac{1}{(x_n-x_2)\cdots(x_n-x_{n+1})}-\frac{1}{(x_n-x_1)\cdots(x_n-x_{n-1})}\right)+$$

$$\frac{f(x_n)}{(x_{n+1}-x_1)\cdots(x_{n+1}-x_n)}=$$

$$\frac{f(x_1)}{(x_1-x_2)\cdots(x_1-x_{n+1})}+\frac{f(x_2)}{x_{n+1}-x_1}\cdot\frac{x_{n+1}-x_1}{(x_2-x_3)\cdots(x_2-x_{n+1})}+\cdots+$$

$$\frac{f(x_{n-1})}{x_{n+1}-x_1}\cdot\frac{x_{n+1}-x_1}{(x_{n-1}-x_1)\cdots(x_{n-1}-x_n)}+\frac{f(x_n)}{(x_n-x_1)\cdots(x_n-x_{n-1})}=$$

$$\frac{f(x_1)}{(x_1-x_2)\cdots(x_1-x_n)}+\frac{f(x_2)}{(x_2-x_1)\cdots(x_2-x_n)}+\cdots+\frac{f(x_n)}{(x_n-x_1)\cdots(x_n-x_{n-1})}$$

故引理对自然数 n 也成立,因而由数学归纳法就证明了引理。

现在利用均差给出插值多项式的另一种表示方法。

定理 11.3.2 设 $f(x)$ 是 x 的任意函数,$x_1,x_2,\cdots,x_n$ 是两两不同的分点,$y_n=f(x_n)$,那么

(1)$f(x)=p_n(x)+R_n(x)$;其中

$$p_n(x)=f(x_1)+f(x_1,x_2)(x-x_1)+\cdots+$$
$$f(x_1,x_2,\cdots,x_n)(x-x_1)\cdots(x-x_{n-1})$$
$$R_n(x)=f(x,x_1,x_2,\cdots,x_n)(x-x_1)\cdots(x-x_n)$$

(2)$L_n(x)=p_n(x)$。

证明 (1)设 x 是任意一点,考虑 x 和$x_1,x_1,x_2,\cdots,x_1,x_2,\cdots,x_n$ 等分点的组构成的均差。由均差的定义就有

$$f(x)=f(x_1)+f(x,x_1)(x-x_1)$$
$$f(x,x_1)=f(x_1,x_2)+f(x,x_1,x_2)(x-x_2)$$
$$f(x,x_1,x_2)=f(x_1,x_2,x_3)+f(x,x_1,x_2,x_3)(x-x_3)$$
$$\vdots$$
$$f(x,x_1,x_2,\cdots,x_{n-1})=f(x_1,x_2,\cdots,x_n)+f(x,x_1,x_2,\cdots,x_n)(x-x_n)$$

把上面各式中的第二式代入第一式即得 $f(x)=p_1(x)+R_1(x)$,其中

$$p_1(x)=f(x_1)+f(x_1,x_2)(x-x_1)$$
$$R_1(x)=f(x,x_1,x_2)(x-x_1)(x-x_2)$$

类似的,将上面各式中的第三式代入 $f(x)=p_1(x)+R_1(x)$ 即得 $f(x)=p_2(x)+R_2(x)$,其中

$$p_2(x)=f(x_1)+f(x_1,x_2)(x-x_1)+$$
$$f(x_1,x_2,x_3)(x-x_1)(x-x_2)$$
$$R_2(x)=f(x,x_1,x_2,x_3)(x-x_1)(x-x_2)(x-x_3)$$

依次类推即可得 $f(x)=p_n(x)+R_n(x)$,其中

$$p_n(x)=f(x_1)+f(x_1,x_2)(x-x_1)+\cdots+$$
$$f(x_1,x_2,\cdots,x_n)(x-x_1)\cdots(x-x_{n-1})$$
$$R_n(x)=f(x,x_1,x_2,\cdots,x_n)(x-x_1)\cdots(x-x_n)$$

(2) 显然 $p_n(x)$ 是一个次数不大于 n 的多项式,并且由上述表达式即可得出

$$p_n(x_k) = f(x_k) = y_k, \quad k = 1,2,\cdots,n$$

因此 $p_n(x)$ 也是一个满足插值多项式问题的解。由插值多项式的唯一性(定理 11.3.1) 即得

$$L_n(x) = p_n(x)$$

这就证明了定理。

具有定理 11.3.2 中形式的插值多项式,计算非常方便,增加一个插值点,只须要多计算一项,而 $P_n(x)$ 的各项系数恰好又是各阶的均差值。通常使用以下的均差表进行计算:

x_k	$f(x_k)$	一阶均差	二阶均差	三阶均差	四阶均差
x_1	$f(x_1)$	$f(x_1,x_2)$			
x_2	$f(x_2)$	$f(x_2,x_3)$	$f(x_1,x_2,x_3)$		
x_3	$f(x_3)$	$f(x_3,x_4)$	$f(x_2,x_3,x_4)$	$f(x_1,x_2,x_3,x_4)$	
x_4	$f(x_4)$	$f(x_4,x_5)$	$f(x_3,x_4,x_5)$	$f(x_2,x_3,x_4,x_5)$	$f(x_1,x_2,x_3,x_4,x_5)$
x_5	$f(x_5)$				

例如如果用这个表格来计算上面已经算过两次的例子就有

x_k	$f(x_k)$	一阶均差	二阶均差
3	3		
2	2	1	
1	1	1	0

因此由均差形式的插值公式立即得到

$$f(x) = f(x_1) + f(x_1,x_2)(x-x_1) + f(x_1,x_2,x_3)(x-x_1)(x-x_2) =$$
$$3 + (x-3) + 0\cdot(x-3)(x-2) = x$$

哈,这不要简单死了。不过不要忘记,在这简单的背后,我们证明定理 11.3.2 时可是费了不少劲,并且使用了均差这个概念,而这个概念又用掉了不少纸张。因此这个表面上的简单实际上是由于定理 11.3.2 已经吸收了一些本质上的困难。但是不管怎么样,这个例子说明均差形式的插值公式在实际计算时的确是很好用的。

对性质更好的函数,我们可以得到比定理 11.3.2 更好的结果。

定理 11.3.3 设 $f(x)$ 存在直至 n 阶的导数,那么

(1) $$f(x_1,x_2,\cdots,x_n) = \frac{f^{(n-1)}(\xi)}{(n-1)!}, \quad x_1 < \xi < x_n$$

(2) $$f(x) = p_n(x) + \frac{f^{(n)}(\xi)}{n!}l(x)$$

其中 $l(x) = (x - x_1)(x - x_2)\cdots(x - x_n), x_1 < \xi < x_n$。

证明 (1) 由定理 11.3.2 知

$$f(x) = p_n(x) + R_n(x)$$

其中 $$R_n(x) = f(x, x_1, x_2, \cdots, x_n)l(x)$$

显然 $R_n(x)$ 在区间$[x_1, x_n]$上有 n 个零点 $x_1, x_2, \cdots, x_n$。同时由于 $f(x)$ 存在直至 n 阶的导数,所以 $R_n(x)$ 也存在直至 n 阶的导数。

在每一个小区间$[x_k, x_{k+1}], k = 1,2,\cdots,n-1$上,由于 $R_n(x_k) = R_n(x_{k+1}) = 0$,故在此每一个小区间上对 $R_n(x)$ 应用罗尔定理即可得出在区间(x_1, x_n)内存在 $n-1$ 个点 $\xi_1^{(1)}, \xi_2^{(1)}, \cdots, \xi_{n-1}^{(1)}$ 使得

$$R_n'(\xi_k^{(1)}) = 0, x_1 < \xi_1^{(1)} < x_2 < \xi_2^{(1)} < \cdots < x_{n-1} < \xi_{n-1}^{(1)} < x_n$$

对 $R_n'(x)$ 和分点 $\xi_1^{(1)}, \xi_2^{(1)}, \cdots, \xi_{n-1}^{(1)}$ 进行和上面同样的论证可以得出在区间$(\xi_1^{(1)}, \xi_{n-1}^{(1)})$内存在 $n-2$ 个分点 $\xi_1^{(2)}, \xi_2^{(2)}, \cdots, \xi_{n-2}^{(2)}$ 使得

$$R_n''(\xi_k^{(2)}) = 0, \xi_1^{(1)} < \xi_1^{(2)} < \xi_2^{(1)} < \xi_2^{(2)} < \cdots < \xi_{n-2}^{(1)} < \xi_{n-2}^{(2)} < \xi_{n-1}^{(1)}$$

将这个过程进行 $R_n(x) = f(x) - p_n(x)$ 到在$(\xi_1^{(n-2)}, \xi_2^{(n-2)})$内存在一点 $\xi = \xi_1^{(n-1)}$ 使得 $R_n^{(n-1)}(\xi_1^{(n-1)}) = 0$。

但是 $R_n(x) = f(x) - p_n(x)$,而

$$p_n(x) = f(x_1) + f(x_1, x_2)(x - x_1) + \cdots + f(x_1, x_2, \cdots, x_n)(x - x_1)\cdots(x - x_{n-1})$$

故对 $R_n(x) = f(x) - p_n(x)$ 两边各求导 $R_n(x) = f(x) - p_n(x)$,再令 $x = \xi$ 即得

$$0 = R_n^{(n-1)}(\xi) = f(\xi) - (n-1)!f(x_1, x_2, \cdots, x_n)$$

由此即得出

$$f(x_1, x_2, \cdots, x_n) = \frac{f^{(n-1)}(\xi)}{(n-1)!}$$

(2) 对 $f(x, x_1, x_2, \cdots, x_n)$ 应用(1)中已证明的结果即得在(x_1, x_n)内存在一点 ξ 使得

$$f(x, x_1, x_2, \cdots, x_n) = \frac{f^{(n)}(\xi)}{n!}$$

将上式代入到 $R_n(x)$ 的表达式中去即得

$$R_n(x) = f(x, x_1, x_2, \cdots, x_n)l(x) = \frac{f^{(n)}(\xi)}{n!}l(x)$$

这就证明了定理。

下面我们来考虑分点间的距离都是相等的特殊情况。

定义 11.3.2

(1) 设 $x_k = x_1 + (k-1)h, k = 1,2,\cdots,n-1, y_k = f(x_k)$,则 $y_{k+1} - y_k$ 称

为 $y = f(x)$ 在点 x_k 处的一阶向前差分，记为 Δy_k；

(2)$\Delta y_{k+1} - \Delta y_k$ 称为 $y = f(x)$ 在点 x_k 处的二阶向前差分，记为 $\Delta^2 y_k$；

(3) 一般的，如果已定义了 $y = f(x)$ 在点 x_k 处的 $n-1$ 阶向前差分 $\Delta^{n-1}y_k$，则称 $\Delta^{n-1}y_{k+1} - \Delta^{n-1}y_k$ 为 $y = f(x)$ 在点 x_k 处的 n 阶向前差分，记为 $\Delta^n y_k$；

向前差分有以下性质：

定理 11.3.4

(1)$\Delta^n y_k = y_{n+k} - C_n^1 y_{n+k-1} + C_n^2 y_{n+k-2} + \cdots (-1)^i C_n^i y_{n+k-i} + \cdots + (-1)^n y_k$；

(2)$f(x_1, x_2, \cdots, x_n) = \dfrac{\Delta^{n-1} y_1}{(n-1)!\, h^{n-1}}$；

(3)$\Delta^n y_1 = h^n f^{(n)}(\xi)$。

证明 (1) 容易用数学归纳法证明，略；

(2)
$$f(x_1, x_2) = \frac{y_2 - y_1}{x_2 - x_1} = \frac{\Delta y_1}{h}$$

$$f(x_1, x_2, x_3) = \frac{f(x_2, x_3) - f(x_1, x_2)}{x_3 - x_1} = \frac{1}{2h}\left(\frac{\Delta y_2}{h} - \frac{\Delta y_1}{h}\right)\frac{\Delta^2 y_1}{2h^2}$$

因此对自然数 $n = 2$ 和 $n = 3$，(2) 中的结论成立，假设对自然数 $n-1$，(2) 中的结论成立，即假设

$$f(x_1, x_2, \cdots, x_{n-1}) = \frac{\Delta^{n-2} y_1}{(n-2)!\, h^{n-2}}$$

那么

$$f(x_1, x_2, \cdots, x_n) = \frac{f(x_2, \cdots, x_{n-1}) - f(x_1, \cdots, x_{n-2})}{x_{n-1} - x_1} =$$

$$\frac{1}{(n-1)h}\left(\frac{\Delta^{n-2} y_2}{(n-2)!\, h^{n-2}} - \frac{\Delta^{n-2} y_1}{(n-2)!\, h^{n-2}}\right) =$$

$$\frac{\Delta^{n-2} y_2 - \Delta^{n-2} y_1}{(n-1)!\, h^{n-1}} = \frac{\Delta^{n-1} y_1}{(n-1)!\, h^{n-1}}$$

因此(2) 中的结论对自然数 n 也成立。因而由数学归纳法就证明了(2)。

(3) 由定理 11.3.3 和(2) 已证明的结论就得到

$$f(x_1, x_2, \cdots, x_n, x_{n+1}) = \frac{f^{(n)}(\xi)}{n!} = \frac{\Delta^n y_1}{n!\, h^n}$$

由此就得出(3)。

定义 11.3.3

(1) 设 $x_k = x_1 + (k-1)h, k = 1, 2, \cdots, n-1, y_k = f(x_k)$，则 $y_{k+1} - y_k$ 称为 $y = f(x)$ 在点 x_{k+1} 处的一阶向后差分，记为∇y_{k+1}；

(2) $\nabla y_{k+1} - \nabla y_k$ 称为 $y = f(x)$ 在点 x_{k+1} 处的二阶向后差分，记为$\nabla^2 y_{k+1}$；

(3) 一般的，如果已定义了 $y = f(x)$ 在点 x_{k+1} 处的 $n-1$ 阶向后差分

$\nabla^{n-1}y_{k+1}$，则称$\nabla^{n-1}y_{k+1}-\nabla^{n-1}y_k$为$y=f(x)$在点$x_{k+1}$处的$n$阶向后差分，记为$\nabla^n y_{k+1}$。

根据向后差分的意义，容易得知，对同一个分点来说，向前差分和向后差分的方向恰好相反。由此易于得出向后差分与向前差分类似的性质。

定理 11.3.5

(1) $\nabla^n y_k = y_k - C_n^1 y_{k-1} + C_n^2 y_{k-2} + \cdots (-1)^i C_n^i y_{k-i} + \cdots + (-1)^n y_{k-n}$；

(2) $f(x_1, x_2, \cdots, x_n) = \dfrac{\nabla^{n-1} y_n}{(n-1)!\,h^{n-1}}$；

(3) $\nabla^n y_{n+1} = h^n f^{(n)}(\xi)$。

利用这些公式，现在我们就可以对第九章中的一个等式给出一个严格的证明了。在第九章9.5中，我们曾经计算$(p-1)^n$的n次差分(注意在第九章9.5中出现的Δ的意义和这里的∇的意义是相同的)。在那里，我们根据观察得出

$$\nabla^n (p-1)^n = n!$$

但是当时并未给予严格的证明。现在我们就可以对此给予一个严格的而且简单得不得了的证明。实际上设$f(x)=x^n$，$x_{n+1}=p-1$，$h=1$，那么利用定理11.3.5(3)中的公式就立刻可以得到

$$\nabla^n (p-1)^n = \nabla^n y_{n+1} = f^{(n)}(\xi) = n!$$

有趣的是如果企图直接证明这一式子可没有这么简单。而且我不知道是否有很简单的直接证法，读者中哪位有不妨发表出来，或告诉作者，让咱们也见识一下。所以数学中有许多东西会在你意想不到的地步出现曲径通幽的妙境。往往两个表面上看起来毫不相干的东西可以发生联系并由此产生出原来所想不到的巧妙解法。

关于插值，还有许多问题，例如带导数的插值等等。我们就到此为止了，有兴趣的读者可以参考专门研究此类问题的计算数学文献。

最后我们来谈一下最小二乘法。之所以要讲这个问题是由于以上我们讲了好多关于插值的问题，其实当初人们研究插值问题主要是想用它来逼近函数，而且历史上有一段时间曾经有些数学家认为只要选取足够多的点进行插值，我们就能够无限精确地逼近一个预定的函数。不过现在这种看法已经被证明是不全面的。最简单的例子就是如果企图用多项式对(0,1)中的函数$y=\dfrac{1}{x}$进行无限精确的逼近是不可能的，而且对这一函数，选取的点越多，所得的插值多项式的性质可能越坏。你只要注意$y=\dfrac{1}{x}$具有性质当$x\to 0$时，$f(x)\to\infty$(称为有限逸时现象)，而任何多项式都不可能有此性质就可以预先大致地估计到，用多项式去逼近这种$f(x)$是不可能有好结果的。

既然对有些函数不可能用多项式去无限地逼近，于是人们就去考虑另外一

个问题，就是对给定的一批数据，如何选取一个次数给定的多项式甚至其他函数，使得逼近的误差最小，这就是最小二乘法要解决的问题。

现在考虑 N 对实验数据 (x_i, y_i)，$i = 1,2,\cdots,N$。我们的目的是要从这些数据找到一个近似的函数关系式 $y = f(x)$。最简单的情况就是设 $f(x)$ 是一个多项式。为确定起见，设此多项式是 m 次的，于是可设

$$y = f(x) = a_0 + a_1 x + \cdots + a_m x^m, m < N$$

如果把点 (x_i, y_i) 代入上述多项式，就会得到 N 个方程。一般来说，在 $m < N$ 时，用 N 个方程去精确地确定 $m+1$ 个未知数是不可能的，有可能会出现互相矛盾的方程。也就是说，上述 N 个等式一般是不可能同时成立的。一般人做到此处就嘎然而止了。既然一般情况下是无解，那就没什么可考虑的了。的确，要是从解方程组去确定系数这一角度去考虑问题，这个问题已没有什么可考虑的了。但是如果换一个角度去考虑那就不一样。因为你反正是要去近似，不能相等就不能相等，即使不能相等也没有关系。不能相等就是说把等式两边相减所得的式子不能为零，能等于0最好，不能等于0，这个差就是误差，所以我们现在不去看等式了，而是看得到的 N 个误差，也就是下面的 N 个式子

$$\begin{aligned} a_0 + a_1 x_1 + \cdots + a_m x_1^m - y_1 &= R_1 \\ a_0 + a_1 x_2 + \cdots + a_m x_2^m - y_2 &= R_2 \\ &\vdots \\ a_0 + a_1 x_N + \cdots + a_m x_N^m - y_N &= R_N \end{aligned}$$

而问题也不是原来的通过解方程去决定系数，而是考虑如何使总的误差最小。总的误差按通常的概念应该就是

$$|R_1| + |R_2| + \cdots + |R_N|$$

但是这个函数的性质不太方便用数学去处理，所以我们现在考虑另一种性质的总误差，那就是

$$\varphi(a_0, a_1, \cdots, a_m) = R_1^2 + R_2^2 + \cdots + R_N^2$$

这个函数用数学处理起来就很方便了，而且如果 φ 很小，那么各个 R_i 肯定也很小，所以用这个 φ 去控制误差是完全合格的。

根据微积分学的知识可知，使得 φ 达到极小的 $a_0, a_1, \cdots, a_m$ 必须适合下面的方程组

$$\begin{aligned} \frac{\partial \varphi}{\partial a_0} &= \frac{\partial R_1^2}{\partial a_0} + \frac{\partial R_2^2}{\partial a_0} + \cdots + \frac{\partial R_N^2}{\partial a_0} = 0 \\ \frac{\partial \varphi}{\partial a_1} &= \frac{\partial R_1^2}{\partial a_1} + \frac{\partial R_2^2}{\partial a_1} + \cdots + \frac{\partial R_N^2}{\partial a_1} = 0 \\ &\vdots \end{aligned}$$

$$\frac{\partial\varphi}{\partial a_m}=\frac{\partial R_1^2}{\partial a_m}+\frac{\partial R_2^2}{\partial a_m}+\cdots+\frac{\partial R_N^2}{\partial a_m}=0$$

先分别计算对每个系数的偏导得出

$$\frac{\partial\varphi}{\partial a_0}=\frac{\partial R_1^2}{\partial a_0}+\frac{\partial R_2^2}{\partial a_0}+\cdots+\frac{\partial R_N^2}{\partial a_0}=2\left(R_1\frac{\partial R_1}{\partial a_0}+R_2\frac{\partial R_2}{\partial a_0}+\cdots+R_N\frac{\partial R_N}{\partial a_0}\right)=$$

$$2\left(\left(\sum_{i=1}^{N}1\right)a_0+\left(\sum_{i=1}^{N}x_i\right)a_1+\cdots+\left(\sum_{i=1}^{N}x_i^m\right)a_m-\sum_{i=1}^{N}y_i\right)$$

$$\frac{\partial\varphi}{\partial a_1}=\frac{\partial R_1^2}{\partial a_1}+\frac{\partial R_2^2}{\partial a_1}+\cdots+\frac{\partial R_N^2}{\partial a_1}=2\left(R_1\frac{\partial R_1}{\partial a_1}+R_2\frac{\partial R_2}{\partial a_1}+\cdots+R_N\frac{\partial R_N}{\partial a_1}\right)=$$

$$2\left(\left(\sum_{i=1}^{N}x_i\right)a_0+\left(\sum_{i=1}^{N}x_i^2\right)a_1+\cdots+\left(\sum_{i=1}^{N}x_i^{m+1}\right)-\sum_{i=1}^{N}x_iy_i\right)$$

$$\vdots$$

$$\frac{\partial\varphi}{\partial a_m}=\frac{\partial R_1^2}{\partial a_m}+\frac{\partial R_2^2}{\partial a_m}+\cdots+\frac{\partial R_N^2}{\partial a_m}=2\left(R_1\frac{\partial R_1}{\partial a_m}+R_2\frac{\partial R_2}{\partial a_m}+\cdots+R_N\frac{\partial R_N}{\partial a_m}\right)=$$

$$2\left(\left(\sum_{i=1}^{N}x_i^m\right)a_0+\left(\sum_{i=1}^{N}x_i^{m+1}\right)a_1+\cdots+\left(\sum_{i=1}^{N}x_i^{2m}\right)-\sum_{i=1}^{N}x_i^my_i\right)$$

为简明起见,设

$$\sum_{i=1}^{N}x_i^k=S_k,\sum_{i=1}^{N}x_i^ky_i=T_k$$

于是上面的方程组就成为

$$\begin{aligned}S_0a_0+S_1a_1+\cdots+S_ma_m&=T_0\\S_1a_0+S_2a_1+\cdots+S_{m+1}a_m&=T_1\\&\vdots\\S_ma_0+S_{m+1}a_1+\cdots+S_{2m}a_m&=T_m\end{aligned}$$

这个方程组有 $m+1$ 个未知数和 $m+1$ 个方程。如果它有唯一解的话,我们就可用多项式

$$y=f(x)=a_0+a_1x+\cdots+a_mx^m$$

来近似地代替数据 $(x_1,y_1),(x_2,y_2),\cdots,(x_N,y_N)$ 所在的曲线。

定理 11.3.6 设 $(x_1,y_1),(x_2,y_2),\cdots,(x_N,y_N)$ 是给定的 N 对数

$$\sum_{i=1}^{N}x_i^k=S_k,\sum_{i=1}^{N}x_i^ky_i=T_k$$

那么当 $N>m$ 时,方程组(I)

$$S_0a_0+S_1a_1+\cdots+S_ma_m=T_0 \qquad ①$$

$$S_1a_0+S_2a_1+\cdots+S_{m+1}a_m=T_1 \qquad ②$$

$$\vdots$$

$$S_ma_0+S_{m+1}a_1+\cdots+S_{2m}a_m=T_m \qquad \textcircled{m+1}$$

存在唯一解。

证明　从线性代数中线性方程组的理论可知，方程组(I)存在唯一解的充分必要条件是相应的齐次方程组(I_0)

$$S_0a_0 + S_1a_1 + \cdots + S_ma_m = 0 \quad ①$$
$$S_1a_0 + S_2a_1 + \cdots + S_{m+1}a_m = 0 \quad ②$$
$$\vdots$$
$$S_ma_0 + S_{m+1}a_1 + \cdots + S_{2m}a_m = 0 \quad (m+1)$$

只有零解。

假设方程组(I_0)存在非零解 $a_0, a_1, \cdots, a_m$，那么将方程组(I_0)中的第一个等式两端都乘以 a_0，第二个等式的两端都乘以 $a_1, \cdots$，第 $m+1$ 个等式的两端都乘以 a_m，然后把所得的 $m+1$ 个等式加起来就得到

$$\begin{aligned}0 = {} & a_0(S_0a_0 + S_1a_1 + \cdots + S_ma_m) + a_1(S_1a_0 + S_2a_1 + \cdots + S_{m+1}a_m) + \cdots + \\ & a_m(S_ma_0 + S_{m+1}a_1 + \cdots + S_{2m}a_m) = \\ & a_0\sum_{j=0}^{m} a_jS_j + a_1\sum_{j=0}^{m} a_jS_{j+1} + \cdots + a_m\sum_{j=0}^{m} a_jS_{j+m} = \\ & \sum_{k=0}^{m} a_k\sum_{j=0}^{m} a_jS_{j+k} = \sum_{k=0}^{m} a_k\sum_{k=0}^{m} a_j\sum_{i=1}^{N} x_i^{j+k} = \\ & \sum_{i=1}^{N}\left(\sum_{k=0}^{m} a_kx_i^k\right)\left(\sum_{j=0}^{m} a_jx_i^j\right) = \sum_{i=1}^{N}(a_0 + a_1x_i + \cdots + a_mx_i^m)^2 = \\ & y_1^2 + y_2^2 + \cdots + y_N^2\end{aligned}$$

由于 $y_1, y_2, \cdots, y_N$ 都是实数，故由 $y_1^2 + y_2^2 + \cdots + y_N^2 = 0$ 就得出

$$y_1 = y_2 = \cdots = y_N = 0$$

这说明 m 次多项式 $y = f(x)$ 有 N 个零点，由于 $N > m$，故由定理 10.1.4 即得 $f(x) \equiv 0$，因而

$$a_0 = a_1 = \cdots = a_m = 0$$

这与$(a_0, a_1, \cdots, a_m)$是方程组(I_0)的非零解的假设矛盾。所得的矛盾就说明(I_0)方程组只有零解，因而方程组(I)有唯一解。

不过我们从微积分学里知道$(a_0^*, a_1^*, \cdots, a_m^*)$是方程组(I)的解只是 $\varphi(a_0, a_1, \cdots, a_m)$ 在$(a_0^*, a_1^*, \cdots, a_m^*)$取得极小值的必要条件和可疑条件。$\varphi(a_0, a_1, \cdots, a_m)$ 是否确实在此处取得极小值还需进一步验证。

定理 11.3.7　设$(x_1, y_1), (x_2, y_2), \cdots, (x_N, y_N)$是给定的 N 对数

$$a_0 + a_1x_1 + \cdots + a_mx_1^m - y_1 = R_1$$
$$a_0 + a_1x_2 + \cdots + a_mx_2^m - y_2 = R_2$$
$$\vdots$$

$$a_0 + a_1 x_N + \cdots + a_m x_N^m - y_N = R_N$$

$$\varphi(a_0, a_1, \cdots, a_m) = R_1^2 + R_2^2 + \cdots + R_N^2$$

$(a_0^*, a_1^*, \cdots, a_m^*)$ 是方程组(I) 的解，那么 $\varphi(a_0, a_1, \cdots, a_m)$ 在$(a_0^*, a_1^*, \cdots, a_m^*)$ 处取到最小值。

证明　设 $F(x) = a_0 + a_1 x + \cdots + a_m x^m$ 是任意 m 次多项式。

$$f(x) = a_0^* + a_1^* x + \cdots + a_m^* x^m$$

$$\delta = \sum_{i=1}^{N} (F(x_i) - y_i)^2 - \sum_{i=1}^{N} (f(x_i) - y_i)^2$$

那么

$$\delta = \sum_{i=1}^{N} (F(x_i)^2 - 2F(x_i) y_i - f(x_i)^2 + 2f(x_i) y_i) =$$

$$\sum_{i=1}^{N} ((F(x_i) - f(x_i))^2 + 2(F(x_i) - f(x_i))(f(x_i) - y_i)) =$$

$$\sum_{i=1}^{N} ((F(x_i) - f(x_i))^2 + 2\sum_{i=1}^{N} (F(x_i) - f(x_i))(f(x_i) - y_i)$$

然而由$(a_0^*, a_1^*, \cdots, a_m^*)$ 是方程组(I) 的解可知

$$\sum_{i=1}^{N} (F(x_i) - f(x_i))(f(x_i) - y_i) =$$

$$\sum_{i=1}^{N} (a_0 - a_0^* + (a_1 - a_1^*) x_i + \cdots + (a_m - a_m^*) x_i^m)(f(x_i) - y_i)$$

$$\sum_{i=1}^{N} \Big(\sum_{i=1}^{m} (a_k - a_k^*) x_i^k \Big)(f(x_i) - y_i) =$$

$$\sum_{k=0}^{m} (a_k - a_k^*) \sum_{i=1}^{N} (f(x_i) - y_i) x_i^k =$$

$$\sum_{k=0}^{m} (a_k - a_k^*) \sum_{i=1}^{N} \frac{\partial R_i^2}{\partial a_k} = \sum_{k=0}^{m} (a_k - a_k^*) \frac{\partial \varphi}{\partial a_k} = 0$$

这就说明 $\varphi(a_0, a_1, \cdots, a_m)$ 确实在$(a_0^*, a_1^*, \cdots, a_m^*)$ 处取到最小值。

以上我们已从理论上论述了用多项式去拟合数据的最小二乘问题是一定有唯一解的。

以前的计算方法教科书讲完以上内容后往往还要举一个拟合数据的例子，不过现在已经绝少有人用手算去求解这类问题了。因为已有了编制得很好的各种软件供人们使用。例如在 Matlab 中，可以使用以下命令来求解最小二乘问题。(凡是前面加 % 号的语句都不是 Matlab 的命令，而是我们对命令的解释)

$x = [x_1, x_2, \cdots, x_N]$　(% 输入数据 $x_1, x_2, \cdots, x_N$)

$y = [y_1, y_2, \cdots, y_N]$　(% 输入数据 $y_1, y_2, \cdots, y_N$)

$p = polyfit(x, y, m)$(% 用 m 次多项式对数据$(x_1, y_1), (x_2, y_2), \cdots, (x_N,$

y_N) 进行拟合)；

当执行上述命令后，Matlab 将给出答案

$p = a_0 \quad a_1 \quad \cdots \quad a_n$ （% 这里 $a_0 \quad a_1 \quad \cdots \quad a_n$ 表示拟合多项式 $a_0x^n + a_1x^{n-1} + \cdots + a_n$ 的各项系数）

你还可以将拟合多项式与原数据进行对比：

$x = a : h : b$ （% 表示用步长 h 对区间 $[a, b]$ 中的点输入）

$y = a_0 * x.\hat{}n + a_1 * x.\hat{}n - 1 + \cdots + a_{n-1} * x + a_n$ （% 注意，二次以上的 x 后面一定要加一个英文的句点.，但是一次项中的 x 后面不加）

plot (x, y) （% 描出多项式 y 的图像）

hold on （% 在输入新的命令时，保持刚才描出的图形不消失）

$$x1 = [x_1, x_2, \cdots, x_N]$$

$$y1 = [y_1, y_2, \cdots, y_N]$$

plot$(x1, y1, 'o')$ （% 描出 $(x_1, y_1), (x_2, y_2), \cdots, (x_N, y_N)$ 并在所描出的点上加 o，此处的 o 在实际上是输入的英文的小写字母 o）

下面是一个输入以上语句后所得图像的实例，其中

$$x1 = [0, 0.1, 0.2, 0.3, 0.4, 0.5, 0.6, 0.7, 0.8, 0.9, 1]$$

（可用命令 $x = 0 : 0.1 : 1$ 代替）

$$y1 = [-0.447, 1.978, 3.28, 6.16, 7.08, 7.34, 7.66, 9.56, 9.48, 9.30, 11.2]$$

用二次多项式进行拟合。

拟合后给出的答案是

$$a_0 = -9.810\,8, a_1 = 20.129\,3, a_2 = -0.031\,7$$

上述的对比图的用处是在有些情况下可以帮助我们发现异常点。所谓异常点就是根据实际数据一般都是连续变化的假设。如果所有的点都在拟合曲线附近，而只有一或两个点明显偏离拟合曲线，那么这一两个点就需要特别研究。这里有两种可能，一种是实际数据本来就是如此，一种是这一两个点是因为某种偶然原因，在测量或记录时发生了明显的误差。至于到底是哪种情况，就需要根据经验和反复再重新采取数据来判断。如果判断

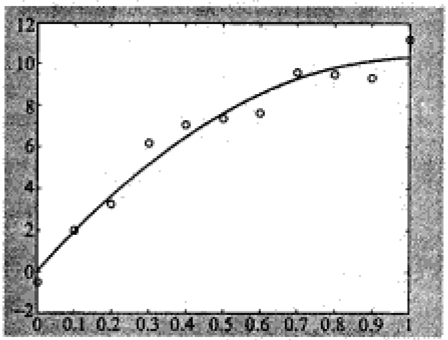


图 11.3.1 在 Matlab 中用二次多项式对数据进行拟合后的对比图
（带 * 的点表示原始数据）

这一两个点确实是异常点，那么把它们从数据中去掉，往往可以得到更好的拟合。但是特别要注意，异常点不能太多，超过三个甚至两个就很难说还是异常点了，更不允许随心所欲地把自己不喜欢的点都当成异常点处理掉，这就不是科学的拟合而是凑数据了。

另外一个问题就是根据直观，一般人都会产生这种想法，即一次拟合不行，我就用二次，仿佛次数越高，效果就越好。但是实际情况不是如此，原因就在于我们虽然已在理论上解决了任意次拟合曲线的存在性，但是实际运用中会发生理论上不考虑的问题。例如理论上可以严格证明平衡点的存在性，然而实际上不稳定的平衡点根本观察不到。用多项式进行最小二乘拟合问题也是如此。实践的结果表明，当次数超过 7 时，如果不提高运算的精度，拟合效果会急剧下降。有的书中用一些数据例子对此作了直观的解释。简单说来就是当次数较大时，方程组(1) 将成为所谓病态的，因而实际计算的性能很差。至于什么是病态的方程组，我们就不多讲了，愿意深入钻研的读者可参看计算方法方面的专著。

最后，我们提一下在实际运用以上方法时的关键是是否能达到实际问题所需要的精度。恰恰是在此最关键的问题上，还没有一般的理论来满足我们的需要。

所谓实际问题一般分为两类。第一类是已有现成的公式，但是太复杂，希望找出合用的近似公式。第二类是只有实际的数据，希望给出能计算这些数据的近似公式。不管是哪一类问题，最后的关键都在你给出的公式算出来的数据的精度是否合乎要求。这是一个硬限制。

但是这里有一个原则，就是近似公式的精度不可能超过原始数据的精度。

下面，我们举一个第一类问题的答案。

例 11.3.1 $erf(x)=\frac{2}{\sqrt{\pi}}\int_0^x e^{-t^2}dt\ (x>0)$ 称为误差函数，在文献 Hastings C. Jr, HaywardJ.T. and Wong J.P. Jr, Approximations for digital computers, Princeton Univ. Press.1955. 中给出了两个近似公式。

(1) $$erf(x)\approx 1-\left(1+\sum_{i=1}^{6}a_ix^i\right)^{-16}$$

其中 $a_1=0.070\,523\,078\,4$, $a_2=0.042\,282\,012\,3$, $a_3=0.009\,270\,527\,2$

$a_4=0.000\,152\,014\,3$, $a_5=0.000\,276\,567\,2$, $a_6=0.000\,043\,063\,8$

以上近似公式的最大绝对误差是 1.3×10^{-7}。

(2) $$erf\left(\frac{x}{\sqrt{2}}\right)\approx 1-\left(1+\sum_{i=1}^{4}a_ix^i\right)^{-4}$$

其中 $a_1=0.196\,854$, $a_2=0.115\,194$, $a_3=0.000\,344$, $a_4=0.019\,527$

以上近似公式的最大绝对误差是 2.5×10^{-4}。

习题 11.3

1. 构造次数尽可能低的插值多项式使得

(1) $f(1) = 2, f(2) = 3, f(3) = 1$;

(2) $f(0.2) = 0.6, f(0,6) = 0.8, f(0.8) = 0.2$。

2. 试求满足条件 $f(x_1) = y_1, f(x_2) = y_2, f(x_3) = y_3$ 且 $f'(x_2) = y'_2$ 的插值多项式，并证明其余项为

$$R(x) = \frac{f^{(4)}(\xi)}{4!}(x - x_1)(x - x_2)^2(x - x_3)$$

3. 利用数值 $x_1 = 1, x_2 = 25, x_3 = 100, y_1 = 1, y_2 = 5, y_3 = 10$ 给出平方根函数 $y = \sqrt{x}(1 \leqslant x \leqslant 100)$ 的近似公式。

4. 利用数值 $\sin 0^\circ = 0, \sin 30^\circ = \frac{1}{2}, \sin 90^\circ = 1$ 给出如下形式的近似公式

$$\sin x^\circ = ax + bx^3, \quad 0 \leqslant x \leqslant 90$$

利用这个公式，求出 $\sin 20^\circ, \sin 40^\circ, \sin 80^\circ$ 给出如下的近似值，并与真值作比较，看所得的近似值的精确度是多少。

5. 设有试验数据如下表所示：

x	1.36	1.49	1.73	1.81	1.95	2.16	2.28	2.48
y	14.094	15.069	16.844	17.378	18.435	19.949	20.963	22.495

用最小二乘法分别求出上述数据的一次及二次拟合函数，并将所得的曲线与原数据作对比。

6. 用三次多项式拟合以下数据

x	4	2	1	0	1	3	4	6
y	35.1	15.1	15.9	8.9	0.1	0.1	21.1	135

7. 用最小二乘法求一个形如 $y = a + bx^2$ 的函数，拟合下列数据

x	19	25	31	38	44
y	19.0	32.3	49.0	73.3	97.8

8. 用二次多项式拟合以下数据

x	0	1	2	3	4	5	6	7	8	9	10
y	3	87	156	210	238	252	239	211	158	90	5

11.4 Logistic 映射周期 3 窗口的参数

从大约 1970 年起，一门叫做混沌学的理论逐渐形成了。其主要令人感兴趣和感到惊异之处在于这一理论告诉人们，在完全是确定性的系统中竟然会表现出类似于随机无序的复杂现象。一开始，连发现这一现象的专家本人都对这一结论感到不可思议。然而随着大量研究成果的出现，当科学界已普遍认识到这决不是一种个别的偶然现象，而是一种在自然界，社会学和经济、气象、生物界等各种极不相同的领域中都普遍存在的事情后，对混沌学的研究就变得极为热门，大量的文献爆炸式地出现。许多科普刊物也热衷于向读者展示这一迷人的题目。自从混沌理论的研究成果被通俗地介绍给大众后，可以说，它已极大地改变了人们对世界的看法。本来从拉普拉斯开始，人们就肯定地认为存在于我们外部的世界可以明确地分成两种本质上完全不同的领域，在一个领域中，是确定性规律在起着作用，而在另一个领域中，是随机性的规律在统治着。而现在人们发现，在这两种如此对立的领域之间已不可能画出一条明确的界限了。这对某些人不啻于说太阳是从西边出来一样。

对混沌学的诞生来说，生态学家们起了特别的作用。生态学家经常使用数学模型，但是他们深知数学模型其实是极其复杂的真实世界的一种简化，因而必然带有局限性。正是生态学家首先发现一些看似合理的数学模型会引出与实际相差甚远的不可思议的结论。

比如说，你想研究某种飞蛾的数量规律，那么第一步就是列出每年的飞蛾数量，例如第一年是 31 000，第二年是 35 000 等等，然后的一个极其自然的想法就是找出第二年的飞蛾数量与第一年的飞蛾数量的一种关系，用数学的语言来说，如果用 y 表示第二年的飞蛾数量，用 x 表示第一年的飞蛾数量，那就是要找出 y 与 x 之间的一种函数关系。

生态学家们，其实任何科学家们的第一步，总是愿意寻求哪怕是一种很粗糙的但是尽可能简单的函数关系。最简单的函数关系就是线性的函数关系了。这种函数关系假定第二年的数量与第一年的数量之间构成一种固定的比例。用数学式子写出来就是假定

$$x_{n+1} = \mu x_n$$

这就是马尔萨斯的不受食物与伦理限制的解决方案。其中 μ 是一个参数，代表群体的增长率，例如 μ 可以是 1.1，那么如果第一年是 10，第二年就是 11。如果输入是 20 000，那么输出便是 22 000，等等。

然而生态学家通过几代的实践最终认识到上面那种线性式的关系顶多只

能暂时用一下，过几年这个关系中的系数便需要修正一下才能使公式符合实际的数据。这只不过是一种比较文雅的说法。说得直白点，这种做法只不过是一种马后炮式的对数据的凑合，用这种公式既不可能对历史作永久的解释，也不可能对未来作任何有价值的预测。在理论上，这一公式的结论只有三种：第一种是 $0 < \mu < 1$ 的情况，这时物种的数量逐年严格地按比例减少，随着时间趋于无穷，物种的数量趋于 0，也就是说，物种趋于灭亡；第二种是 $\mu = 1$ 的情况，这时物种的数量保持精确的不变，这在实践中是不可能的；第三种就是 $\mu > 1$ 的情况，这时物种的数量逐年严格地按比例增加，随着时间趋于无穷，物种的数量趋于无穷。这当然也是不可能的。于是按此公式在实践中唯一可能的结局就是一切物种都趋于死灭。多么悲哀的结局！本来阳光灿烂，充满生气的真实世界在此公式的眼光里，甚至连英国著名文学家莎士比亚剧中人物哈姆雷特式的“生或是死”的悲剧式的选择都没有，而只有世界末日的一条黑路。

实际的情况是，当物种的数量增加到一定程度后，由于食物等各种因素的限制，它的数量就会自动降下来，而当物种数量下降到一定程度后，在外界条件不变的情况下，由于生活条件的改善(因为没有那么多生物争夺资源了)，物种的数量又会自动增多而最后达到一种平衡。为此，生态学家对原来的马尔萨斯公式给出了一种修正的方案，即在原来的公式中增加一项因式 $1 - x$，也就是说，修正后的公式为

$$x_{n+1} = \mu x_n(1 - x_n)$$

这新增加的因式使得物种的增长自动成为有界，因为当 x_n 增加时，$1 - x_n$ 便会减少。这便是所谓的逻辑斯梯公式。它也可以写成

$$x_{n+1} = f(x_n)$$

其中

$$f(x) = \mu x(1 - x)$$

如果单考察函数 $f(x) = \mu x(1 - x)$，它是再简单不过了，一条开口向下的对称抛物线而已，在 $x = \frac{1}{2}$ 时取到最大值，其他就没什么好说的了，不过如此而已。这是任何一个中学生都知道的事情。然而当生态学家和数学家在混沌理论的研究热潮中再回过头来看这个函数时，竟发觉它包含有不可思议的复杂性和令人匪夷所思的丰富内容。

问题在于公式 $x_{n+1} = f(x_n)$ 的含义不在于单独的研究二次函数 $f(x) = \mu x(1 - x)$ 本身，而是把此函数作反复的乃至无穷的迭代，并且要连同参数 μ 的变化考虑在内。现在人们已经认识到非线性的无穷次作用一般就必然会产生复杂性，而参数的变化会对复杂性的形式增加许多花样，如分支、倍周期分支、混沌等等。

现在我们就来看看迭代 $x_{n+1} = \mu x_n(1 - x_n)$ 会产生什么出人意料的现象。

读者手边最好有一个计算器，当然如果有计算机，并且机器中加装了如 Matlab 这样可以编程序的软件那就更好了，利用计算器或计算机可以作数值“试验”。选定一个 μ 值之后，对于一个初值 x_0，按照程序 $x_{n+1}=\mu x_n(1-x_n)$ 不断地按执行键，计算器(机)就会显示出 $x_1,x_2,\cdots$ 等，而后就可归纳分析结果。

我们还可以采用下述的作图方法来观察和大致研究迭代的过程。

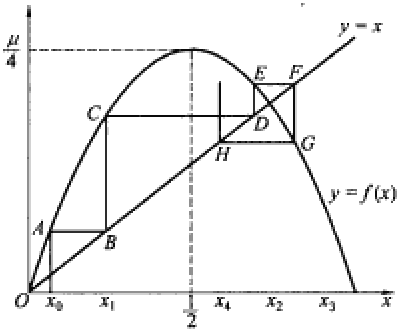


图 11.4.1

在 xy 平面上画出曲线 $y=f(x)$ 和第一象限的角平分线 $y=x$。对于初值 x_0，作竖直线 $x=x_0$ 与曲线交于点 A，于是 A 的纵坐标是 $f(x_0)$ 即 x_1，由 A 作平行于 x 轴的水平线 AB 交角平分线于 B，于是点 B 的横坐标就是 x_1。类似地，相继一横一竖在曲线和角平分线之间来回作 $BC,CD,DE,EF,EG,GH,\cdots$ 等各线段，于是 D,F,H 各点的横坐标分别是 $f(x_1)=x_2, f(x_2)=x_3, f(x_3)=x_4$ 等(图 11.4.1)。这种作图方法精度当然比计算器(机)差得多，在精确分析时不能采用，但比较直观，便于说明问题。

下面我们来看使 μ 从小到大会发生什么结果。

(1) 当 $0<\mu\leqslant 1$ 时，在区间 $[0,1]$ 内抛物线和角平分线只有一个交点 $x=0$(图 11.4.2)。如果 x_0 就是 0，那么以后 $x_1,x_2,x_3,\cdots$ 显然都是 0。所以 0 是一个平衡点或者不动点。如果 x_0 不等于 0，那么 $0<x_0\leqslant 1$，因此 $0\leqslant 1-x_0<1$，于是

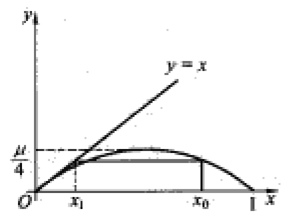


图 11.4.2　当 $0<\mu\leqslant 1$ 时有一个稳定平衡点

$$0<x_1=\mu x_0(1-x_0)<(\mu(1-x_0))x_0<1$$

$$0<x_2=\mu x_1(1-x_1)<x_1<1$$

$$\vdots$$

$$0<x_{n+1}=\mu x_n(1-x_n)<x_n<1$$

$$\vdots$$

于是
$$0<\cdots<x_{n+1}<x_n<\cdots<x_1<x_0<1$$

即叙列 $\{x_n\}$ 是严格递减有下界的。因此根据维尔斯特拉斯收敛原理可知当 $n\to\infty$ 时，x_n 必定趋于某个有限的极限 ξ。在迭代关系

$$x_{n+1}=\mu x_n(1-x_n)$$

中令 $n\to\infty$ 就得到

$$\xi = \mu\xi(1-\xi)$$

由于当 $0 < \mu \leqslant 1$ 时，上面的方程只有唯一解 $\xi = 0$。因此我们就得出当 $0 < \mu \leqslant 1, n \to \infty$ 时，对任意 $0 < x_0 \leqslant 1$ 有 $x_n \to 0$。这时我们说，这个平衡点 $x = 0$ 是稳定的。读者如果用计算器做实验就可发现，不管在[0,1]初值是什么，经过足够多的迭代后，显示的数字就是稳定平衡值0了。

(2) 当 $1 < \mu < 3$ 时，抛物线和角平分线交于两点(图 11.4.3) $x = \xi_1$ 和 $x = \xi_2$。其中 $\xi_1 = 0$，$\xi_2 = 1 - \frac{1}{\mu}$，即迭代 $x_{n+1} = \mu x_n(1-x_n)$ 有两个平衡点，其中 ξ_1 是原先($\mu < 1$)时就有的，但现在它是不稳定的。只要初值 x_0 稍微偏离它(一个任意小的正数)，那么以后 x_n 就回不到 ξ_1 的附近。与它相反，新出现的平衡点 ξ_2 确是稳定的。根据一个称为克尼格定理的结果，为了确信这一点只要计算抛物线在 ξ_2 处的斜率即可。如果斜率的绝对值小于 1，就说明它是稳定的，大于1则是不稳定的。所以不论初值 x_0 是什么，除了 x_0 恰好为0之外，经过多次迭代，计算器显示的结果总是 ξ_2(用数学的语言来说就是，在区间[0,1]中，除了一个0测集外，对几乎所有的初值 x_0，x_n 都收敛到 ξ_2)。

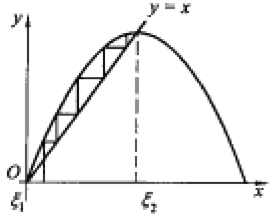


图 11.4.3　当 $1 < \mu < 3$ 时有两个平衡点，一个稳定，一个不稳定

综合以上的结果，可以把平衡点数值和参数 μ 的关系画成图 11.4.4，其中虚线表示不稳定，即实际上是观察不到的。在 $\mu = 1$ 处出现了分支(bifurcation，也可译成分歧，分叉)现象，即原来的一个平衡点 $x = 0$ 在经过 $\mu = 1$ 时突然变成了两个 $x = \xi_1 = 0$ 和 $x = \xi_2 = 1 - \frac{1}{\mu}$(也可以这样描述分支的特性，即当 $\mu \to 1$ 时有 $\xi_1 \to 0$ 和 $\xi_2 \to 0$)。但是稳定的平衡点仍然只有一个。

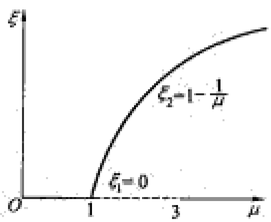


图 11.4.4　平衡点的分支现象

当 $3 < \mu < 1 + \sqrt{6}$ 时，容易算出在抛物线和角平分线的两个交点处斜率的绝对值都大于1，因而两个平衡点都不稳定。用计算器实验时，显示的数字不会趋于一个固定的值。但是可以发现，经过多次迭代以后，显示的数字总是交替为两个数字。比如取 $\mu = 3.2$，经过多次迭代(初值不取0，也不取0.687 5)，取小数点后4位数字显示结果，就可以看到

$$0.513\,0,\ 0.799\,5,\ 0.513\,0,\ 0.799\,5,\cdots$$

可以验证这两点都满足关系式 $x_{n+2} = x_n$，它们代表了一个周期为2的周期解，或简称为周期2解。平衡点可以看成是周期为1的周期解。周期2解可以用分析式表达出来。

$$x_{n+2} = f(x_{n+1}) = \mu x_{n+1}(1 - x_{n+1}) = \mu^2 x_n(1 - x_n)(1 - \mu x_n(1 - x_n))$$

因此 x_{n+2} 是 x_n 的4次多项式。如果令 $x_{n+2} = x_n$，就得到一个4次方程。这个4次方程的其中两个根就是上面所说的 $\xi_1 = 0$ 和 $\xi_2 = 1 - \frac{1}{\mu}$（它们同时是周期1解），而另外两个是新增加的平衡点。

$$\xi_3, \xi_4 = \frac{1}{2\mu}(1 + \mu \mp \sqrt{(\mu + 1)(\mu - 3)})$$

如取初值为 ξ_3 或 ξ_4，迭代的结果就是周期2解 $\xi_3, \xi_4, \xi_3, \xi_4 \cdots$ 或 $\xi_4, \xi_3, \xi_4, \xi_3$ 或写成

$$\xi_3 \rightleftarrows \xi_4$$

通过分析迭代式

$$x_{n+2} = f(x_{n+1}) = \mu x_{n+1}(1 - x_{n+1}) = \mu^2 x_n(1 - x_n)(1 - \mu x_n(1 - x_n))$$

右端在 ξ_3 或 ξ_4 或处导数的绝对值可以证明当 $3 < \mu < 1 + \sqrt{6}$ 时，ξ_3 或 ξ_4 是稳定的，即除去一个0测集外（就是集合 $\{\xi_1, \xi_2\}$），对几乎所有[0,1]中的初值，x_n 最终都会无限地接近周期2解 $\xi_3 \rightleftarrows \xi_4$。图11.4.5表示 $\mu = 3.2$ 的情况。这种稳定的周期解（周期不等于1）也叫做极限环。当 $\mu \to 3$ 时，$\xi_3 \to \xi_2, \xi_4 \to \xi_2$。因此按照分支说法就是当 μ 增加并通过3时，平衡点 ξ_2 分支成周期2解 $\xi_3 \rightleftarrows \xi_4$，如图11.4.6所示。

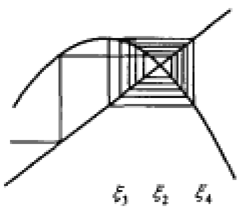


图11.4.5 $\mu = 3.2$ 时的极限环

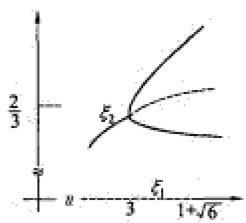


图11.4.6 由平衡点分支出周期2解

现在设 $1 + \sqrt{6} \leqslant \mu < 3.569\ 96$ 时，那么当 μ 跨过 $1 + \sqrt{6}$ 时，周期2解就由原来的稳定突然变成不稳定，多次迭代后，计算其显示一直在四个值 $\xi_5, \xi_6, \xi_7, \xi_8$ 的轮换中循环变化。

$$\xi_5 \to \xi_6 \to \xi_7 \to \xi_8 \to \xi_5$$

它们都是方程 $x_{n+4} = x_n$ 的解（但又不满足 $x_{n+2} = x_n$）。所以这是一个真正的周期4解。当 μ 继续增加到大约3.544 8并跨越此值时，周期4解又突然失去稳定性并分支出周期8解。以后，当 μ 再增加时，原来的稳定周期解又突然失稳，并分支出周期16解，周期32解，周期64解，… 这种周期不断加倍的分支过

程称为倍周期分支。我国古代文献《列子.说符篇》中有这样的话:“歧路之中又有歧焉,吾不知所之 …” 设想如果你沿着上面的参数和平衡点之间的分支图向前走去,不正是进入了这样一种境地了吗?但是这里奇妙的地方在于,这一歧中有歧的过程虽然是无限的,但是这一过程所对应的参数的增长却是有限的。于是根据维尔斯特拉斯原理,对应于这一过程的参数 μ 必递增地趋近于某一极限 μ_∞。更加奇妙的是如果设存在 2 周期解的参数区间的长度为 Δ_2,即 $\Delta_2 = 1 + \sqrt{6} - 3 = \sqrt{6} - 2$,存在 4 周期解的参数区间的长度为 Δ_4,存在 8 周期解的参数区间的长度为 Δ_8,等等,那么当 $n \to \infty$ 时,数列

$$\frac{\Delta_2}{\Delta_4}, \frac{\Delta_4}{\Delta_8}, \frac{\Delta_8}{\Delta_{16}}, \cdots$$

将趋于一个有限的极限 $\delta = 4.669\ 20$。有的读者可能会问,有极限就有极限吧,不是很多式子都会有极限吗?这又有什么奇妙之处呢?这里的奇妙之处在于,这个 $\delta = 4.669\ 20\cdots$ 是一个普适的常数,称为费根鲍姆常数。什么叫普适常数呢?答案是对相当一类表达式与逻辑斯梯映射不同的单峰函数,上述分支过程都会出现,并且当 $n \to \infty$ 时,相应的参数区间的长度的比都趋于这个费根鲍姆常数。这就有点不可思议了。因为这个极限本来是由具体的迭代函数 $f(x)$ 来确定的,结果最后才发现,这个极限竟然与 $f(x)$ 无关,这个事情在事前是难以预料的。那么知道了这个费根鲍姆常数有什么用呢?用处之一就是可以预言什么时候会出现分支。这个道理很简单。因为$\frac{\Delta_{2^n}}{\Delta_{2^{n+1}}} \to \delta$,而 $\Delta_{2^{n+1}} = \mu_{2^{n+1}} - \mu_{2^n}$,因此当 n 充分大时 $\mu_{2^{n+1}}$ 就大致等于

$$\mu_{2^n} + \frac{\Delta_{2^n}}{\delta} = \mu_{2^n} + \frac{\mu_{2^n} - \mu_{2^{n-1}}}{\delta} = \left(1 + \frac{1}{\delta}\right)\mu_{2^n} - \frac{\mu_{2^{n-1}}}{\delta}$$

也就是说,我们有近似公式

$$\mu_{2^{n+1}} \approx \mu'_{2^{n+1}} = \mu_{2^n} = \frac{\mu_{2^n} - \mu_{2^{n-1}}}{\delta} = \left(1 + \frac{1}{\delta}\right)\mu_{2^n} - \frac{\mu_{2^{n-1}}}{\delta}$$

通过数值计算,我们可以得到表 11.4.1。

表 11.4.1　逻辑斯梯映射的倍周期分支值

k	μ_k	Δ_k
1	3.000 000 000 0	
2	3.449 489 742 8	0.449 489 742 8
4	3.544 090 350 6	0.094 600 607 8
8	3.564 407 266 1	0.020 316 915 5
16	3.568 759 419 6	0.004 352 155 3
32	3.569 691 609 8	0.000 932 190 2
64	3.569 891 259 4	0.000 199 649 4

现在我们用上面所说的近似公式来计算 μ_k 的近似值μ_k'，并与真正的 μ_k 值对比，得到表 11.4.2。

表 11.4.2　μ_k 的近似值 μ_k'

k	μ_k	μ_k'
1	3.000 000 000 0	
2	3.449 489 742 8	
4	3.544 090 350 6	3.545 756 679 9
8	3.564 407 266 1	3.564 350 903 6
16	3.568 759 419 6	3.568 758 527 1
32	3.569 691 609 8	3.569 691 517 9
64	3.569 891 259 4	3.569 891 256 3

这下你就可以看出这个费根鲍姆常数的厉害了，因为 μ_k 是不好算的，要是给你和另一个人一人发一个计算器，让你们去算这个 μ_k，而那个人只知道 μ_k 的定义，估计他当时就得傻眼了，算这个 μ_k 没有一台计算机以及合适的软件，估计除了 μ_1，μ_2 外是根本算不出来的。但是算这个 μ_k' 就很简单，只用到加减乘除，用一个手持的计算器就可进行，而且算出来的精度并不差。第一次就精确到小数点后两位。

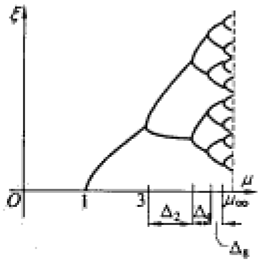


图 11.4.7　逻辑斯梯映射的倍周期分支示意图

这种歧中有歧的情景在 μ 达到$\mu_\infty = 3.569\,944\cdots$ 时，全部周期为 2 的幂次的解就都出现了。如图11.4.7 所示(图中只画出稳定解，而且没有按比例画)。

最后，设 $3.569\,944 < \mu \leqslant 4$。当 μ 再增加，将出现周期不是 2 的幂次的解。以最终 $\mu = 4$ 的为例，这时迭代的表达式为

$$x_{n+1} = 4x_n(1 - x_n)$$

利用三角学中的倍角公式不难验证存在以下两个周期为 3 的周期解。

$$\sin^2 20^\circ \rightarrow \sin^2 40^\circ \rightarrow \sin^2 80^\circ \rightarrow \sin^2 20^\circ$$

$$\sin^2\left(\frac{180^\circ}{7}\right) \rightarrow \sin^2\left(\frac{360^\circ}{7}\right) \rightarrow \sin^2\left(\frac{720^\circ}{7}\right) \rightarrow \sin^2\left(\frac{180^\circ}{7}\right)$$

在一维动力系统中(上面的迭代就是一个由映射定义的离散的一维动力系统)周期 3 解的出现是一件大事情。因为在 1964 年一个叫沙尔科夫斯基

(Шарковский) 的苏联数学家证明了如果把全体自然数排成以下的沙尔科夫斯基次序(符号 $\prec$ 读作前于)

$$3 \prec 5 \prec 7 \prec 9 \prec \cdots \prec \cdots \prec 2 \cdot 3 \prec 2 \cdot 5 \prec 2 \cdot 7 \prec \cdots \prec$$
$$2^2 \cdot 3 \prec 2^2 \cdot 5 \prec 2^2 \cdot 7 \prec \cdots \prec 2^5 \prec 2^4 \prec 2^3 \prec 2 \prec 1$$

那么对于一个[0,1] 区间上的连续映射 $f(x)$ 来说,如果 $m \prec n$,并且迭代

$$x_{n+1} = f(x_n)$$

具有周期 m 解,那么上述迭代就必也具有周期 n 解。但是不一定具有在 m 之前的数为周期的解。由于在沙尔科夫斯基序中,3 是排在头一个位置的数,由沙尔科夫斯基定理就推出,如果迭代 $x_{n+1} = f(x_n)$ 有周期3解,那么它就有任意周期的解。所以这个周期3就是所有周期解的总根子,这就是为什么周期3解那么重要的原因。这些周期解还可能不止一组,例如周期20解就有52 377组。1975年美国华裔数学家李天岩和美国数学家约克(Li and Yorke) 在美国数学月刊上发表了一篇文章,题目是《周期 3 意味着混沌》(《Periodic 3 implies chaos》) 在世界上引起轰动。这篇文章的内容分两部分,其中一部分等于重新证明了沙尔科夫斯基的结果。另一部分结果证明如果系统出现周期 3 解,那么系统中就存在一条行为十分怪异的轨道,它可以距离任意周期轨道任意近(从这点上看,它应该算是比较有规律的),但是这条轨线上又无论什么时候都有距离可以最大程度远的两个点(从这点来看,它又毫无规律)。总体来说,这条轨线是出现在一个规律完全确定的系统中的,但是它的行为却又有许多随机系统才有的性质,比如刚才所说的它可以在整个相空间中"乱跑",因而它的行为是难以"预测" 的,这个难以预测表现在这个数列对于初值的误差十分"敏感",也就是说,两个相差极为微小的初值经过多次迭代后,相互之间的差别可以很大,以至两个相应的数列的性质可能根本不同。这可以在计算器的数值实验中观察到,对于 $\mu = 4$,将 $\sin^2 20°$ 作为 $\sin^2 20°$ 初值输入,因为是一个无理数,不可能用有限小数表示出来,所以你输入的 $\sin^2 20°$ 对于计算器来说肯定是有一定误差的,经过多次迭代后,这个误差被放大到极为显著的地步,以至你得到的将不是

$$\sin^2 20° \longrightarrow \sin^2 40° \longrightarrow \sin^2 80° \longrightarrow \sin^2 20°$$

这个周期解,而是整个[0,1] 区间,也就是说,只偏离周期轨道任意小的一条轨道成为一条在[0,1] 区间中遍历的轨线。这当然是性质完全不同的两种轨道。

以上是逻辑斯梯映射迭代所表现出的种种性质。稳定的平衡点,稳定的周期解(极限环) 都称为吸引子(attactor),这是因为,其他的轨线不论初值如何(除了一个0测集之外),最后都要被"吸引" 到吸引子附近。在逻辑斯梯系统中,除了以上两种吸引子外,还有一种奇异吸引子(strange attractor)。说它奇异,是因为奇异吸引子的几何结构十分复杂,它的内部有许多空洞,但是又不是一个

0测集，另外它的维数不一定像通常的几何形体那样是一个整数，而可能是一个无穷小数。这种现象称为分维。

以上我们只是用通俗的语言描述了一下混沌理论中可能会遇到的一些现象。这算是走马观花吧！但是在科学的大观园中，如果只是走马观花，那还是不够的。对于那些真正想走进科学殿堂的人，还要知道如何把事情严格地说清楚，并给予严格的证明，才能使别人承认你的探索结果。下面我们就对周期3解产生的参数和奇异吸引子的结构两个问题给予严格的叙述。

上面我们已经说明了周期3的出现是一件十分重要的事情，既然如此，一个特别有兴趣的问题就产生了。那就是系统何时出现周期3解，也就是要问，当参数 μ 取什么值时，系统会从本来没有周期3解的状态突然变成有周期3解了。另外一个与此相关的问题是，我们知道，新出现的分支一开始都是稳定的(因此才能被实际观察到)，但是后来当新的分支出现时，老的分支就要失稳，那么我们因此就还要问，这个周期3解产生后，在什么时候失稳，也就是要问当参数 μ 取什么值时，原来稳定的周期3解突然不稳定了。

设 $f_\mu(x) = \mu x(1-x)$，那么我们有

引理 11.4.1 迭代 $x_{n+1} = \mu x_n(1-x_n)$ 存在3周期解的充分必要条件是方程

$$g_3(x) = \frac{f_\mu(f_\mu(f_\mu(x))) - x}{f_\mu(x) - x} = 0$$

存在实根。

证明 迭代 $x_{n+1} = \mu x_n(1-x_n)$ 的周期1点即不动点 x 显然满足方程

$$g_1(x) = f_\mu(x) - x = 0$$

类似的，迭代 $x_{n+1} = \mu x_n(1-x_n)$ 的周期3解必须满足方程

$$f_\mu(f_\mu(f_\mu(x))) - x = 0$$

但是由于所有的周期1解也同时是周期3解，因此 $f_\mu(x) - x = 0$ 的根都是 $f_\mu(f_\mu(f_\mu(x))) - x = 0$ 的根，故

$$f_\mu(x) - x \mid f_\mu(f_\mu(f_\mu(x))) - x$$

因而真正的3周期解必须满足方程

$$g_3(x) = \frac{f_\mu(f_\mu(f_\mu(x))) - x}{f_\mu(x) - x} = 0$$

反过来，满足上述方程的 x 显然满足方程 $f_\mu(f_\mu(f_\mu(x))) - x = 0$ 但是不满足方程 $f_\mu(x) - x = 0$，因而必是迭代 $x_{n+1} = \mu x_n(1-x_n)$ 的周期3解。这就证明了引理。

引理 11.4.2 设 $y = -\mu x$，则

$$g(y) = y^6 + (3\mu+1)y^5 + (3\mu^2+4\mu+1)y^4 + (\mu^3+5\mu^2+3\mu+1)y^3 +$$

$$(2\mu^3+3\mu^2+3\mu+1)y^2+(\mu^3+2\mu^2+2\mu+1)y+\mu^2+\mu+1$$

那么
$$g_3(x)=g(y)$$

因而 $g_3(x)=\dfrac{f_\mu(f_\mu(f_\mu(x)))-x}{f_\mu(x)-x}=0$ 有实数解的充分必要条件是 $g(y)=0$ 有实数解。

证明 令 $y=-\mu x$，那么由计算可知 $g_3(x)=g(y)$，这就证明了引理。

引理 11.4.3 $g(y)=0$ 或没有实根或有 3 个不同的实根或有 6 个不同的实根。

证明 由引理 11.4.1 知 $g_3(x)$ 的实根 x^* 必是 $x_{n+1}=f_\mu(x_n)$ 的 3 周期解以及如果 x^* 是 $x_{n+1}=f_\mu(x_n)$ 的 3 周期解，则 $f_\mu(x^*)$ 和 $f_\mu(f_\mu(x^*))$ 也是 $x_{n+1}=f_\mu(x_n)$ 的 3 周期解，因而再由引理 11.4.1 可知 $f_\mu(x^*)$ 和 $f_\mu(f_\mu(x^*))$ 也必是 $g_3(x)$ 的实根，且这 3 个根必是两两不等的(否则它们就不是真正的 3 周期解而是不动点了，而不动点已从方程 $g_3(x)$ 的根中排除出去了)，就得出 $g_3(x)$ 的实根的个数必是 3 的倍数，而由于 $g_3(x)$ 是 6 次的，故 $g_3(x)$ 的实根的个数只能是 0 或 3 或 6，再由引理 11.4.2 就得出引理。

引理 11.4.4 μ_3 是 $x_{n+1}=f_\mu(x_n)$ 的 3 周期解的分支值(即在 μ_3 的左侧 $x_{n+1}=f_\mu(x_n)$ 不存在 3 周期解，而在包括 μ_3 的另一侧，$x_{n+1}=f_\mu(x_n)$ 存在 3 周期解)的充分必要条件是当 $\mu=\mu_3$ 时，$g(y)=0$ 恰有 3 个不相等的二重根。

证明 由引理 11.4.3 可知 μ_3 是 $x_{n+1}=f_\mu(x_n)$ 的 3 周期解的分支值的充分必要条件是当 $\mu=\mu_3$ 时，$g(y)=0$ 恰有 3 个不相等的实根(因为根据引理 11.4.3 可知 $g(y)=0$ 的实根的个数从无到有的分界点恰好是 3)。从可能性来看，这 3 个不同的实根可能有以下几种情况：

(1)3 个两两不同的单根；

(2) 一个单实根，两个实重根；

(3) 两个单实根，一个实重根；

(4)3 个实二重根。

由于 $g(y)=0$ 是实系数多项式，因而它的复根是两两共轭，成对出现的，故情况(1) 不可能出现。由于一个二重的实根经过参数的一个充分小的扰动可以变成两个实根或没有实根，因而(2)，(3) 两种情况在参数的充分小的扰动下，将会出现和引理 11.4.3 相矛盾的情况。故只可能出现情况(4)。这就证明了引理。

定理 11.4.1 迭代 $x_{n+1}=\mu x_n(1-x_n)$，$\mu>0$ 的周期 3 解的分支值是

$$\mu_3=1+\sqrt{8}=3.828\,427\,124\,746\cdots$$

证明 由计算可知

$$g(y)=(y^3+py^2+qy+r)^2+(\mu^2-2\mu-7)(\beta_2y^2+\beta_1y+\beta_0)$$

其中

$$p = \frac{3\mu + 1}{2}$$

$$q = \frac{3\mu^2 + 10\mu + 3}{8}$$

$$r = \frac{-\mu^3 + 7\mu^2 + 5\mu + 5}{16}$$

$$\beta_2 = \frac{3\mu^3 - 6\mu - 5}{64}$$

$$\beta_1 = \frac{3\mu^3 - 5\mu^2 - 7\mu - 7}{64}$$

$$\beta_0 = \frac{-\mu^4 + 12\mu^3 - 22\mu^2 - 20\mu - 33}{256}$$

注意 $\mu > 0$,由此可知 $g(y) = 0$ 恰有 3 个不同的二重根的必要条件是

$$\mu^2 - 2\mu - 7 = 0$$

或

$$\mu = \frac{2 + \sqrt{32}}{2} = 1 + \sqrt{8}$$

而当 $\mu = 1 + \sqrt{8}$ 时,通过计算可以验证 $g(y) = 0$ 的确恰有 3 个不同的二重根

$$y_1 = \frac{2\sqrt{7}}{3}\cos\left(\frac{1}{3}\arccos\frac{1}{2\sqrt{7}} + \frac{2\pi}{3}\right) + \frac{2 + 3\sqrt{2}}{3} = 0.612\,275\,9\cdots$$

$$y_2 = \frac{2\sqrt{7}}{3}\cos\left(\frac{1}{3}\arccos\frac{1}{2\sqrt{7}} + \frac{4\pi}{3}\right) + \frac{2 + 3\sqrt{2}}{3} = 1.969\,171\,6\cdots$$

$$y_3 = \frac{2\sqrt{7}}{3}\cos\left(\frac{1}{3}\arccos\frac{1}{2\sqrt{7}}\right) + \frac{2 + 3\sqrt{2}}{3} = 3.661\,193\,2\cdots$$

因此由引理 11.4.4 即得

$$\mu_3 = 1 + \sqrt{8}$$

由此定理立即得出:

定理 11.4.2 当 $0 < \mu < 1 + \sqrt{8}$ 时,$g(y)$ 是正定的,即恒有 $g(y) > 0$,当 $0 < \mu < 1 + \sqrt{8}$ 且 $\mu \to 1 + \sqrt{8}$ 时,$\min\limits_{-\infty < x < \infty} g(y) \to 0$。

定理 11.4.2 纯粹是一个代数的结果,但是为了得到它,我们刚才却绕了一个大弯,通过考虑迭代 $x_{n+1} = \mu x_n(1 - x_n)$,$\mu > 0$ 的周期 3 解的分支值才得到这一结果。作者很感兴趣是否能直接证明这一结论。证明这一命题的困难是 $g(y)$ 有性质:当 $\mu \to 1 + \sqrt{8}$ 时,$\min\limits_{-\infty < x < \infty} g(y) \to 0$。因此当 μ 越接近 $1 + \sqrt{8}$ 时,下界的估计就越困难,而 $g(y)$ 的下界的精确值是依赖于 $g(y)$ 的根的,但是这个根我们又无法用解析式子把它表达出来。读者如能直接证明这一命题我认为

就相当于给出了迭代 $x_{n+1} = \mu x_n(1 - x_n), \mu > 0$ 的周期 3 解的分支值的一个直接证明，这是有发表价值的。并希望通告作者(可发邮件到 fby@amss.ac.cn)。

下面来考虑迭代 $x_{n+1} = \mu x_n(1 - x_n), \mu > 0$ 的周期 3 解的失稳条件。

引理 11.4.5 任何一个周期 3 叙列 $x_1, x_2, x_3, \cdots, x_n, \cdots$ 可用通项公式

$$x_n = a + \beta\omega^n + \bar{\beta}\bar{\omega}^n$$

表出。其中 $\omega = \dfrac{-1 + i\sqrt{3}}{2}$，$a$ 是一个实数，$\beta = b + ci$ 是一个复数。

证明 显然 ω 具有特性 $\omega^3 = \bar{\omega}^3 = 1$。

设序列 $x_1, x_2, x_3, \cdots, x_n, \cdots$ 具有通项公式 $x_n = a + \beta\omega^n + \bar{\beta}\bar{\omega}^n$。那么

$$x_{n+3} = a + \beta\omega^{n+3} + \bar{\beta}\bar{\omega}^{n+3} = a + \beta\omega^n\omega^3 + \bar{\beta}\bar{\omega}^n\bar{\omega}^3 = a + \beta\omega^n + \bar{\beta}\bar{\omega}^n = x_n$$

因此叙列 $x_1, x_2, x_3, \cdots, x_n, \cdots$ 是 3 周期的。

反之，假设叙列 $x_1, x_2, x_3, \cdots, x_n, \cdots$ 是 3 周期的。令

$$a + \beta\omega + \bar{\beta}\bar{\omega} = x_1$$

$$a + \beta\omega^2 + \bar{\beta}\bar{\omega}^2 = x_2$$

$$a + \beta\omega^3 + \bar{\beta}\bar{\omega}^3 = a + \beta + \bar{\beta} = x_3$$

并把 a, b, c 看成未知数，那么容易证明上面的关于 a, b, c 的三元一次方程组有唯一解。因此根据上面已经证明的结论就有 $x_4 = x_1, x_5 = x_2, x_6 = x_3, \cdots$ 因而叙列 $x_1, x_2, x_3, \cdots, x_n, \cdots$ 具有通项公式 $x_n = a + \beta\omega^n + \bar{\beta}\bar{\omega}^n$。

引理 11.4.6 设在参数 μ 下迭代存在 $x_{n+1} = \mu x_n(1 - x_n), \mu > 0$ 周期 3 解，并且 $x_n = a + \beta\omega^n + \bar{\beta}\bar{\omega}^n$ 是此周期 3 解构成的叙列的通项公式，那么

$$a = \frac{3\mu + 1 \pm \sqrt{\mu^2 - 2\mu - 7}}{6\mu}$$

证明 把 $x_n = a + \beta\omega^n + \bar{\beta}\bar{\omega}^n$ 代入 $x_{n+1} = \mu x_n(1 - x_n), \mu > 0$ 中，并比较两边的同类项系数(在化简合并同类项时，利用等式 $\omega^2 = \bar{\omega}, \bar{\omega}^2 = \omega$)就得到如下方程组

$$2\beta\bar{\beta} = \left(1 - \frac{1}{\mu}\right)a - a^2$$

$$\bar{\beta}^2 = \left(1 - 2a - \frac{\omega}{\mu}\right)\beta$$

$$\beta^2 = \left(1 - 2a - \frac{\bar{\omega}}{\mu}\right)\bar{\beta}$$

把上面的方程组中的后两式相乘，就得到

$$|\beta|^2 = \left|1 - 2a - \frac{\omega}{\mu}\right|^2 = (1 - 2a)^2 + \frac{1 - 2a}{\mu} + \frac{1}{\mu^2}$$

将此式代入上面的方程组中的第一个式子，并将 a 解出来就得到

$$a = \frac{3\mu + 1 \pm \sqrt{\mu^2 - 2\mu - 7}}{6\mu}$$

由于使得 a 有意义的最小的 μ 的值是 $\mu_3 = 1 + \sqrt{8}$，所以我们又重新得到了定理 11.4.1。

定理 11.4.3 迭代 $x_{n+1} = \mu x_n(1 - x_n), \mu > 0$ 的周期 3 解的失稳参数是

$$\mu_{3u} = 1 + \sqrt{\frac{11}{3} + \sqrt[3]{\frac{1\,915}{54} + \frac{5\sqrt{201}}{2}} + \sqrt[3]{\frac{1\,915}{54} - \frac{5\sqrt{201}}{2}}} =$$

$$3.841\,499\,007\,543\cdots$$

证明 设 $D(\mu)$ 是迭代 $x_{n+1} = \mu x_n(1 - x_n), \mu > 0$ 的周期 3 解的迭代函数 $x_{n+1} = f_\mu(f_\mu(f_\mu(x_n))), y = f_\mu(f_\mu(f_\mu(x_n)))$ 在 $x = x_n$ 处的导数。利用求导数的锁链法则就得出

$$D(\mu) = f_\mu'(f_\mu(f_\mu(x_n)))f_\mu'(f_\mu(x_n))f_\mu'(x_n) =$$
$$\mu(1 - 2x_{n+2})\mu(1 - 2x_{n+1})\mu(1 - 2x_n) =$$
$$\mu^3(1 - 2x_{n-1})(1 - 2x_{n-2})(1 - 2x_{n-3}) = \cdots =$$
$$\mu^3(1 - 2x_1)(1 - 2x_2)(1 - 2x_3)$$

设
$$A = x_1 + x_2 + x_3$$
$$B = x_1x_2 + x_2x_3 + x_3x_1$$
$$C = x_1x_2x_3$$

那么
$$D(\mu) = \mu^3(1 - 2A + 4B - 8C)$$

利用引理 11.4.5 即设 $x_n = a + \beta\omega^n + \bar{\beta}\bar{\omega}^n$，我们就得出

$$A = 3a, \quad B = 3(a^2 - |\beta|^2)$$

由 $x_{n+1} = \mu x_n(1 - x_n)$ 得出

$$\frac{x_{n+1}}{x_n} = \mu(1 - x_n)$$

在上式中令 $n = 1,2,3$，将所得的式子相乘，并利用 $x_4 = x_1$ 就得到

$$1 = \mu^3(1 - x_1)(1 - x_2)(1 - x_2) = \mu^3(1 - A + B - C)$$

由此就得出

$$C = 1 - A + B - \frac{1}{\mu^3}$$

把上式，$A = 3a$ 和 $B = 3(a^2 - |\beta|^2)$ 代人到

$$D(\mu) = \mu^3(1 - 2A + 4B - 8C)$$

中并经过化简就得到

$$D(\mu) = \mu(2 - \mu)\sqrt{\mu^2 - 2\mu - 7} - (\mu^2 - 2\mu - 8)$$

（在得出上式时，由于我们要讨论的是稳定的周期 3 解的失稳现象，因此通过计

算导数，容易确定 $a = \frac{3\mu + 1 - \sqrt{\mu^2 - 2\mu - 7}}{6\mu}$ 对应了稳定的3周期解，而 $a = \frac{3\mu + 1 - \sqrt{\mu^2 - 2\mu - 7}}{6\mu}$ 则对应了不稳定的周期3解。因而在上面的计算中，我们应取根号前带负号的 a。）

在上面我们利用求 $y = f_\mu(f_\mu(f_\mu(x)))$ 的不动点的方法来得出周期3解的分支值 μ_3。μ_3 还必须满足另一个条件，即切分支条件，也就是说，当 $\mu = \mu_3$ 时，$y = f_\mu(f_\mu(f_\mu(x)))$ 恰好与第一象限的角平分线 $y = x$ 相切，因而当 $\mu = \mu_3$ 时应有 $D(\mu) = 1$。因为我们已经用两种方法求出了 $\mu = \mu_3$，所以我们就不再去解方程 $D(\mu) = 1$ 了。但是这一方法同样可以讨论稳定周期3解的失稳参数 μ_{3u}，即完全类似的我们有当 $\mu = \mu_{3u}$ 时，应有 $D(\mu) = -1$。把 $D(\mu) = -1$ 中的根号去掉就得到 μ_{3u} 应满足6次方程

$$H(\mu) = \mu^6 - 6\mu^5 + 4\mu^4 + 24\mu^3 - 14\mu^2 - 36\mu - 81 = 0$$

作变换 $\mu = 1 + t$，我们得到

$$H(1 + t) = H(1 - t) = t^6 - 11t^4 + 37t^2 - 108$$

再令 $t^2 = s$，那么上述方程就成为一个3次方程，此3次方程有唯一实数解

$$s = \frac{11}{3} + \sqrt[3]{\frac{1\,915}{54} + \frac{5\sqrt{201}}{2}} + \sqrt[3]{\frac{1\,915}{54} - \frac{5\sqrt{201}}{2}}$$

由此就得出了周期3解的失稳参数为

$$\mu_{3u} = 1 + t = 1 + \sqrt{s}$$

11.5　三次方程的解法和判据

一般的3次方程的形式为

$$a_0x^3 + a_1x^2 + a_3x + a_4 = 0, a_0 > 0$$

我们先来做一些常规性的化简工作，以使方程化为本质上相同但形式上较为简单的方程。

先用 a_0 去除方程的两边，得出

$$x^3 + b_1x^2 + b_2x + b_3 = 0$$

其中 $$b_1 = \frac{a_1}{a_0}, b_2 = \frac{a_2}{a_0}, b_3 = \frac{a_3}{a_0}$$

再令 $$x = y - \frac{b_1}{3}$$

则方程化为 $$y^3 + py + q = 0$$

其中 $$p = b_2 - \frac{b_1^2}{3}, q = b_3 - \frac{1}{3}b_1b_2 + \frac{2b_1^3}{27}$$

化到这，就要靠些联想了。事实上 $y^3 + py + q = 0$ 这种形式已经和我们经常见的，用的有些东西很相像了，如果你中学数学弄得很熟，那至少有两个东西是很像 $y^3 + py + q = 0$ 的。现在我先讲第一个，那就是完全立方公式

$$(u+v)^3 = u^3 + 3u^2v + 3uv^2 + v^3$$

有的人可能会说，这不像啊。也对，现在这么写是有点不像，不过你可以把它写成

$$(u+v)^3 = u^3 + v^3 + 3uv(u+v)$$

或 $$(u+v)^3 - 3uv(u+v) - (u^3+v^3) = 0$$

你再把上式和 $$y^3 + py + q = 0$$

一比，如果还看不出来他们像在哪，那你老先生这眼力可就有点跟不上了。因为在这两个式子里，y 和 $u+v$，p 和 $-3uv$，q 和 $-(u^3+v^3)$ 显然是1—1对应的东西。这种相似性让我们想到令

$$y = u+v, p = -3uv, q = -(u^3+v^3)$$

那么通过检验即可知道 y 一定是方程 $y^3 + py + q = 0$ 的解。于是现在解原来的方程的问题已经转化为求 u, v 的问题了。即解方程组

$$u^3 + v^3 = -q$$

$$uv = -\frac{p}{3}$$

的问题了。

上面方程组中的第二个3次方就得到

$$u^3 + v^3 = -q$$

$$u^3v^3 = -\frac{p^3}{27}$$

因此 u^3 和 v^3 是二次方程

$$z^2 + qz - \frac{p^3}{27} = 0$$

的根。

由于我们的目的是求出 y 而不是解方程组，又由于 u^3, v^3 是对称的，因此我们可任意指定 u^3 代表此二次方程的哪一个根。不妨设

$$u^3 = \alpha, v^3 = \beta$$

其中

$$\alpha = \frac{-q + \sqrt{q^2 + \frac{4p^3}{27}}}{2} = \frac{1}{2}\left(-q + \sqrt{q^2 + \frac{4p^3}{27}}\right) = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$$

$$\beta=-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}$$

方程 $u^3=z_1$ 和 $v^3=z_2$ 各有3个根，它们分别是$\sqrt[3]{z_1}$，$\sqrt[3]{z_1}\omega$，$\sqrt[3]{z_1}\omega^2$ 和$\sqrt[3]{z_2}$，$\sqrt[3]{z_2}\omega$，$\sqrt[3]{z_2}\omega^2$，其中

$$\omega=\frac{-1+\mathrm{i}\sqrt{3}}{2}$$

方程 $u^3=z_1$ 和 $v^3=z_2$ 的根搭配起来共有9种可能，但是显然并不是每一种搭配都是方程 $y^3+py+q=0$ 的解。因为使得能够成为方程 $y^3+py+q=0$ 的解必须受到条件

$$u^3+v^3=-q$$

$$uv=-\frac{p}{3}$$

的限制，根据 u,v 的定义，它们总是满足 $u^3+v^3=-q$ 这一条件的，因此我们只须检验哪一种搭配满足限制条件 $uv=-\frac{p}{3}$ 即可。经过检验，不难发现只有 $y_1=\alpha+\beta$，$y_2=\alpha\omega+\beta\omega^2$ 和 $y_3=\alpha\omega^2+\beta\omega$ 才是正确的搭配。因此我们就得出：

定理 11.5.1　三次方程 $y^3+py+q=0$ 的三个根可以分别表示为

$$y_1=z_1+z_2$$

$$y_2=\omega z_1+\omega^2 z_2$$

$$y_3=\omega^2 z_1+\omega z_2$$

其中　$z_1=\sqrt[3]{-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}$，$z_2=\sqrt[3]{-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}$

这一公式称为卡丹公式。

历史上，一次方程和二次方程在远古就已经解出。高于二次的方程则耗费许多古代数学家的心血而始终没有解法。直到十六世纪初的意大利文艺复兴时代，一般的三次方程的解法才被意大利数学家斯奇波·德·菲洛得出。按照当时的风气，菲洛的解法没有发表，但是却向他的一个学生讲过。菲洛死后，这个学生凭借此秘密向当时的意大利的一个最大的数学家塔尔塔里雅发起挑战。挑战的内容是要他解出一系列的三次方程。塔尔塔里雅起而应战，并且用八天的时间结束了这场竞赛。在这八天的时间内，他得出了形如 $y^3+py+q=0$ 的任何三次方程的解法，并最后在两小时内解决了对手提出的所有问题。米兰的数学和物理教授卡丹(1501—1576)在得知塔尔塔里雅的发明后，央求塔尔塔里雅将秘诀告诉他。塔尔塔里雅经不住卡丹的苦苦央求，终于同意了，但是前提是卡丹要答应绝对地保守秘密。卡丹当时信誓旦旦地向塔尔塔里雅保证绝对不会泄密，然而后来却背弃了诺言而将塔尔塔里雅的结果发表在他自己的著作《大法

塔尔塔里雅(Tartaglia, Nicolò, 1499—1557)，意大利数学家、军事科学家.原名丰坦那，生于意大利北部布雷西亚，卒于威尼斯.

(Art magna)》里。虽然三次方程的解法公式应该称为塔尔塔里雅公式甚至菲洛公式(但是菲洛的工作由于保密，至今无人见到)，但是由于历史的原因，直到现在为止，仍然把它叫做卡丹公式。

下面我们来讨论一下实系数三次方程 $y^3+py+q=0$。为此我们首先用原始的三次方程 $a_0x^3+a_1x^2+a_3x+a_4=0, a_0>0$ 的系数来表示出卡丹公式中平方根号下的表达式。由直接计算可得

$$\frac{q^2}{4}+\frac{p^3}{27}=\frac{1}{4}\left(b_3-\frac{1}{3}b_1b_2+\frac{2b_1^3}{27}\right)^2+\frac{1}{27}\left(b_2-\frac{b_1^2}{3}\right)^3=$$

$$\frac{1}{108}(27b_3^2-18b_1b_2b_3+4b_1^3b_3-b_1^2b_2^2+4b_2^3)=$$

$$\frac{1}{108a_0^4}(27a_0^2a_3^2-18a_0a_1a_2a_3+4a_1^3a_3-a_1^2a_2^2+4a_0a_2^3)$$

经与三次多项式 $a_0x^3+a_1x^2+a_3x+a_4$ 的判别式对比(见第五章)，我们就得出：

引理 11.5.1 设三次多项式为 $a_0x^3+a_1x^2+a_3x+a_4, a_0>0$，它的判别式为 D，且

$$b_1=\frac{a_1}{a_0}, b_2=\frac{a_2}{a_0}, b_3=\frac{a_3}{a_0}$$

$$p=b_2-\frac{b_1^2}{3}, q=b_3-\frac{1}{3}b_1b_2+\frac{3b_1^3}{27}$$

那么

$$\frac{q^2}{4}+\frac{p^3}{27}=-\frac{D}{108a_0^4}$$

下面我们开始讨论实系数三次方程 $y^3+py+q=0$。

(i) $\frac{q^2}{4}+\frac{p^3}{27}>0$。这时卡丹公式的平方根号下是一个正实数，所以每一个立方根号下面的表示式都是实数。根据我们对根号的约定，当根号表示一个实数时，它就表示根号下那个数的算术根，而奇次方根的算术根就是它本身。因此

$$y_1=z_1+z_2$$

表示一个实数。由于显然 $z_1\neq z_2$，因此 y_2, y_3 都是复数(因为在它们的虚部中，i 的系数是 $\frac{\sqrt{3}}{2}(z_1-z_2)$ 或 $-\frac{\sqrt{3}}{2}(z_1-z_2)$ 都不等于0)，并且由于 $\bar{\omega}=\omega^2, \overline{\omega^2}=\omega$，因此易于验证 $\bar{y}_1=y_2, \bar{y}_2=y_1$。故在这种情况下方程 $y^3+py+q=0$ 有一个实数根和一对共轭复根。

(ii) $\frac{q^2}{4}+\frac{p^3}{27}=0$。这时 $z_1=z_2=\sqrt[3]{-\frac{q}{2}}$，另外还有 $\omega+\omega^2=-1$，故此时有

$$y_1=2z_1, y_2=y_3=-z_1$$

也就是说，这时方程 $y^3+py+q=0$ 的三个根都是实数，并且有重根(当 $z_1\neq 0$ 时是二重根，当 $z_1=0$ 时是三重根)。

(iii) $\frac{q^2}{4}+\frac{p^3}{27}<0$。这时卡丹公式的平方根号下是一个负实数，所以每一个立方根号下面的表示式都是复数。根据我们对根号的约定，当根号表示一个复数时，这个根号是多值的(在这里是三值的)。

设 $z_1=u+vi$，那么

$$z_2=-\frac{p}{3z_1}=-\frac{p\bar{z}_1}{3z_1\bar{z}_1}=-\frac{p}{3(u^2+v^2)}(u-vi)$$

又由 z_1,z_2 的定义可知 z_1^3 和 z_2^3 是互相共轭的，而显然 $(u-vi)^3$ 也是与 z_1^3 共轭的。然而一个复数的共轭数是唯一的，由此就得出

$$z_2^3=\left(-\frac{p}{3(u^2+v^2)}\right)^3(u-vi)^3=(u-vi)^3$$

$$\left(-\frac{p}{3(u^2+v^2)}\right)^3=1$$

上式中左边是一个实数的立方，而立方等于1的实数只有1本身，因此就得出

$$z_2=u-vi=\bar{z}_1$$

再由 $\bar{\omega}=\omega^2,\overline{\omega^2}=\omega$ 就得出 $\overline{\omega z_1}=\bar{\omega}\bar{z}_1=\omega^2z_2,\overline{\omega^2z_1}=\overline{\omega^2}\bar{z}_1=\omega z_2$ 就可知

$$y_1=z_1+z_2$$

$$y_2=\omega z_1+\omega^2z_2$$

$$y_3=\omega^2z_1+\omega z_2$$

中每个数都是两个互相共轭的复数之和，因此都是实数。而由引理11.5.1又可知 y^3+py+q 的判别式不等于0，因此这三个根都不相等。即在这种情况下方程 $y^3+py+q=0$ 有三个不相等的实根。

由上面的讨论就得出

定理 11.5.2 实系数三次方程 $y^3+py+q=0$。

当 $\frac{q^2}{4}+\frac{p^3}{27}>0$ 时，有一个实数根和一对共轭复根；

当 $\frac{q^2}{4}+\frac{p^3}{27}=0$ 时，有三个实根，并且其中有两个根或三个根相等；

当 $\frac{q^2}{4}+\frac{p^3}{27}<0$ 时，有三个不相等的实根。

由定理11.5.2，引理11.5.1和例5.3.3就又重新得出定理10.3.6(2)。

定理 11.5.3 在实系数三次方程 $f(x)=a_0x^3+a_1x^2+a_3x+a_4=0$，$a_0>0$ 中，设

$$D=a_1^2a_2^2-4a_1^3a_3-4a_0a_2^3+18a_0a_1a_2a_3-27a_0^2a_3^2$$

那么

当 $D<0$ 时，$f(x)$ 有一个实数根和一对共轭复根；

当 $D = 0$ 时，$f(x)$ 有三个实根，并且其中有两个根或三个根相等；

当 $d > 0$ 时，$f(x)$ 有三个不相等的实根。

上面我们既给出了实系数三次方程的求解公式，又对它进行了完整的讨论，如此关于三次方程，似乎已没有什么问题可再讨论了。然而还有一个问题在古代曾困扰过一些数学家，这个问题即使在现代，对于刚开始了解三次方程解法的人来说，一开始也可能会感到困惑。这就是比如对于方程

$$(x-1)(x-2)(x-3) = x^3 - 6x^2 + 11x - 6 = 0$$

虽然你明明知道它有三个实根 $x_1 = 1, x_2 = 2$ 和 $x_3 = 3$，但是用卡丹公式得出的值是一个形式上的等式，而不是一个可以直接进行计算的通常意义下的公式。于是人们自然想到，对于这种三次方程，是否能得出一个"实"的公式。其实，"实"的公式是有的，但是这个问题之所以能困扰人，是由于所有感到困扰的人在企图得出一个所谓"实"的公式的时候，都在心里有一个没有说出来的期望，这个期望说明白了，就是希望能得出一个根号下是实数的，由各种根号组成的公式。这个希望现在已知是不可能的。这种三次方程具有三个不同实根的情况称为不可约情况。不过要严格证明这一结论，要用到更复杂的理论，比如拉格朗日、阿贝尔和伽罗华理论，这些理论可是一两句话讲不清楚的。

其实每一个在历史上困惑过人们的问题，都在于人们预先在心里对这个问题有一种不正确的设想和期望，等到这个问题解决了，人们才会发现，原来的设想和期望根本不符合实际情况，一旦人们认识到，这就是事情的本来面目，就不会对这个问题再感到困惑了。比如你习惯于认为只有正数，实数才有意义，那你一开始对于负数和复数自然会感到不可理解；如果你预先认为世界上所有的量都应该是"有理"的，那么当你知道还有无理数存在时，自然会感到震惊，如果你想当然地以为连续函数是很好的函数，自然应该是可微的，那么当别人告诉你还存在着处处连续但是处处不可微的函数时，你必然会感到不可思议。在三次方程的求解公式问题上也是如此，很多人根据二次方程的情况就认为三次方程就应该也有一种类似的公式，结果按照这种思路去考虑问题，而白白地耗费了时间和精力。而当你认识到事情的本来面目就是对于具有三个不同实根的三次方程来说，本来就不存在你原来以为存在的那种公式时，你就一点也不会感到有什么奇怪、不可思议或迷惑不解了。

虽然如此，即使对认识到事情本来面目的人来说，仍然会感到有些别扭。原因就在于，我明明知道解是什么，却没有一个能算出解来的公式。对高次方程来说，事情就是这样，不过对于三次方程来说，实际上是可以推导出这样的公式来的，但是这个公式如上所说，当然不可能是由根号组成的。下面我们就来推导不可约情况下三次方程的求解公式。这个解法的基础是观察到

$$y^3 + py + q = 0$$

与三倍角公式 $$\cos 3\theta = 4\cos^3\theta - \cos\theta$$

或 $$4\cos^3\theta - 3\cos\theta - \cos 3\theta = 0$$

或 $$\cos^3\theta - \frac{3}{4}\cos\theta - \frac{1}{4}\cos 3\theta = 0$$

的类似性。(在推导卡丹公式时，我们曾利用了$(u+v)^3 - 3uv(u+v) - (u^3+v^3) = 0$与$y^3+py+q=0$的类似性，当时我们曾说如果你中学数学弄得很熟，那至少有两个东西是很像$y^3+py+q=0$的。这第二个类似于$y^3+py+q=0$的东西就是三倍角公式)

你现在把p看成$-\frac{3}{4}$，把q看成$-\frac{1}{4}\cos 3\theta$，把y看成$\cos\theta$，那$\cos^3\theta - \frac{3}{4}\cos\theta - \frac{1}{4}\cos 3\theta = 0$就变成了$y^3+py+q=0$。

不过这样看还是有问题，首先p肯定不能只等于$-\frac{3}{4}$，另外把y看成$\cos\theta$就已默认了y是满足限制$|y|\leqslant 1$的，这也不符合实际情况。为去除这些问题，我们可以在

$$\cos^3\theta - \frac{3}{4}\cos\theta - \frac{1}{4}\cos 3\theta = 0$$

的两边乘以一个正的参变量λ^3以增加自由度。这样上式就成为

$$\lambda^3\cos^3\theta - \frac{3}{4}\lambda^3\cos\theta - \frac{1}{4}\lambda^3\cos 3\theta = 0$$

现在我们可模仿上面的做法而令

$$y = \lambda\cos\theta,\ -\frac{3}{4}\lambda^2 = p,\ -\frac{1}{4}\lambda^3\cos 3\theta = q$$

于是上面这个等式就变成了

$$y^3 + py + q = 0$$

于是我们立刻看出，只要通过等式$-\frac{1}{4}\lambda^3\cos 3\theta = q$求出$\theta$，再通过等式$y = \lambda\cos\theta$就可以求出$y$了。不过有些细心的读者可能会注意到，刚才我们还有一个式子没有用，就是$-\frac{3}{4}\lambda^2 = p$，而这个式子决定了$p$不能大于0，因此他们会问，要是$p>0$怎么办。问得好，不过别忘了，我们现在是在不可约条件下讨论问题(如果方程属于可约情况，我们就不需要如此讨论，直接应用卡丹公式即可)。这时我们有以下结果保证$p<0$。

引理 11.5.2 如果$\frac{q^2}{4}+\frac{p^3}{27}<0$，那么必有

(1)$p<0$；

(2)$\left|\frac{3\sqrt{3}q}{2p\sqrt{-p}}\right|<1$。

证明 (1) 由$\frac{q^2}{4}+\frac{p^3}{27}<0$得出$p^3<-\frac{27}{4}q^2<0$,因此$p<0$。

(2) 由$\frac{q^2}{4}+\frac{p^3}{27}<0$得出$\frac{q^2}{4}<-\frac{p^3}{27}$,因此$\left|\frac{q}{2}\right|<\frac{-p\sqrt{-p}}{3\sqrt{3}}$,由此就得出

$$\left|\frac{3\sqrt{3}q}{2p\sqrt{-p}}\right|=\left|\frac{3\sqrt{3}q}{-2p\sqrt{-p}}\right|<1$$

因此,现在我们可以放心大胆地进行推导了,由$-\frac{3}{4}\lambda^2=p$得出

$$\lambda=\sqrt{-\frac{4p}{3}}=2\sqrt{-\frac{p}{3}}$$

将此式代入$-\frac{1}{4}\lambda^3\cos 3\theta=q$即得

$$\cos 3\theta=-\frac{4q}{\lambda^3}=-\frac{4q}{8\left(\sqrt{-\frac{p}{3}}\right)^3}=\frac{3\sqrt{3}q}{2(-p)\sqrt{-p}}=\frac{3\sqrt{3}q}{2p\sqrt{-p}}$$

由引理 11.5.2 可知$\cos 3\theta$是有意义的。因而

$$\theta=\theta_k=\frac{1}{3}\arccos\left(\frac{3\sqrt{3}q}{2p\sqrt{-p}}\right)+\frac{2k\pi}{3},\quad k=0,1,2$$

而方程$y^3+py+q=0$的解为

$$y_k=2\sqrt{-\frac{p}{3}}\cos\theta_k,\quad k=1,2,3$$

由上面的讨论就得出不可约情况下实系数三次方程的求解公式。

定理 11.5.4 设$\frac{q^2}{4}+\frac{p^3}{27}<0$,$\theta_k=\frac{1}{3}\arccos\left(\frac{3\sqrt{3}q}{2p\sqrt{-p}}\right)+\frac{2k\pi}{3}$,$k=0,1,2$,那么实系数三次方程$y^3+py+q=0$的三个不同的实数解为

$$y_k=2\sqrt{-\frac{p}{3}}\cos\theta_k,\quad k=1,2,3$$

例 11.5.1 解方程$x^3+3x^2-6x+4=0$。

解 令$x=y-1$,则$y^3-9y+12=0$,于是有$p=-9,q=12$。

$$\Delta=\frac{q^2}{4}+\frac{p^3}{27}=\frac{12^2}{4}-\frac{9^3}{27}=36-27=9$$

$$z_1=\sqrt[3]{-\frac{q}{2}+\sqrt{\Delta}}=\sqrt[3]{-\frac{12}{2}+\sqrt{9}}=\sqrt[3]{-6+3}=-\sqrt[3]{3}$$

$$z_1=\sqrt[3]{-\frac{q}{2}+\sqrt{\Delta}}=\sqrt[3]{-\frac{12}{2}-\sqrt{9}}=\sqrt[3]{-6-3}=-\sqrt[3]{9}$$

$$y_1=z_1+z_2=-\sqrt[3]{3}-\sqrt[3]{9}$$

$$y_2=\omega z_1+\omega^2z_2=\frac{\sqrt[3]{3}+\sqrt[3]{9}}{2}+\frac{\sqrt{3}\sqrt[3]{9}-\sqrt{3}\sqrt[3]{3}}{2}\mathrm{i}$$

$$y_2 = \omega^2 z_1 + \omega z_2 = \frac{\sqrt[3]{3}+\sqrt[3]{9}}{2} - \frac{\sqrt{3}\sqrt[3]{9}-\sqrt{3}\sqrt[3]{3}}{2}\mathrm{i}$$

$$x_1 = y_1 - 1 = -1-\sqrt[3]{3}-\sqrt[3]{9}$$

$$x_2 = y_2 - 1 = \frac{-2+\sqrt[3]{3}+\sqrt[3]{9}}{2} + \frac{\sqrt{3}\sqrt[3]{9}-\sqrt{3}\sqrt[3]{3}}{2}\mathrm{i}$$

$$x_3 = y_3 - 1 = \frac{-2+\sqrt[3]{3}+\sqrt[3]{9}}{2} - \frac{\sqrt{3}\sqrt[3]{9}-\sqrt{3}\sqrt[3]{3}}{2}\mathrm{i}$$

例 11.5.2 解方程 $x^3-6x^2+9x-3=0$。

解 令 $x=y+2$,则 $y^3-3y-1=0$。$p=-3,q=-1$。

$$\Delta = \frac{q^2}{4}+\frac{p^3}{27} = \frac{1}{4}-\frac{3^3}{27} = -\frac{3}{4}$$

$$\frac{3\sqrt{3}q}{2p\sqrt{-p}} = \frac{-3\sqrt{3}}{2(-3)\sqrt{3}} = \frac{1}{2}$$

$$\arccos\left(\frac{3\sqrt{3}q}{2p\sqrt{-p}}\right) = \arccos\frac{1}{2} = 60°, \frac{1}{3}\cdot 60° = 20°$$

$$\theta_1 = 20° + \frac{2\pi}{3} = 20° + 120° = 140°$$

$$\theta_2 = 20° + \frac{2\cdot 2\pi}{3} = 20° + 240° = 260°$$

$$\theta_1 = 20° + \frac{2\cdot 3\pi}{3} = 20° + 360° = 380°$$

$$y_1 = 2\sqrt{-\frac{p}{3}}\cos\theta_1 = 2\cos 140°$$

$$y_2 = 2\sqrt{-\frac{p}{3}}\cos\theta_2 = 2\cos 260°$$

$$y_3 = 2\sqrt{-\frac{p}{3}}\cos\theta_3 = 2\cos 380°$$

$$x_1 = y_1+2 = 2+2\cos 140° = 2(1+\cos 140°) = 4\cos^2 70° = 4\sin^2 20°$$

$$x_2 = y_2+2 = 2+2\cos 260° = 2(1+\cos 260°) = 4\cos^2 130° = 4\sin^2 40°$$

$$x_3 = y_3+2 = 2+2\cos 380° = 2(1+\cos 380°) = 4\cos^2 190° = 4\sin^2 80°$$

习题 11.5

1.解下列方程

(1)$x^3-6x+9=0$ (2)$x^3+12x+63=0$

(3)$x^3+9x^2+18x+28=0$ (4)$x^3+6x^2+30x+25=0$

(5)$x^3-6x+4=0$ (6)$x^3+6x+2=0$

2.解方程:$x^3-6x^2+6x-2=0$。

3. 解方程：$x^3-7x^2+14x-7=0$。

4. 解方程：$x^3-(2+3\sqrt{2})x^2+(5+4\sqrt{2})x-(3+\sqrt{2})=0$。

5. 解方程：$x^3-(2-3\sqrt{2})x^2+(5-4\sqrt{2})x-(3-\sqrt{2})=0$。

6. 解方程：$x^3-3abx+a^3+b^3=0$。

7. 解方程：$x^3-(a+b+c)x^2+(ab+bc+ac)x-abc=0$。

8. 得出求方程 $x^5-5ax^3+5a^2x-2b=0$ 的根的代数公式。

11.6 四次多项式零点的完全判据和正定性条件

在第十章定理 10.3.6(2) 和第十一章定理 11.5.3 中我们用两种不同的方法都得出了三次方程的判别条件，但是在第十一章中得出这一判据的方法可比在第十章中绕弯得多。在第十一章中，我们是先研究了如何解一般的三次方程，然后得出了卡丹公式，最后才得出了根的判别条件。而在第十章中，我们是根据判别式的定义直接得出这一结论的。对比之下，就会觉得，如果不是为了还要得到其他东西，绕这么大的一个弯子，得出来的结论竟和别人下一个定义就可直接得出来的结论一样实在有点不值得，同时也就会觉得，判别式这个概念还是很厉害的。

因此在讨论四次方程时，我们就想直接由判别式入手。不过为了满足有些读者的欲望，我们还是先讲一下四次方程的解法。

一般的四次方程

$$a_0x^4+4a_1x^3+6a_2x^2+4a_3x+a_4=0,a_0>0$$

一定可以化为

$$x^4+4b_1x^3+6b_2x^2+4b_3x+b_4=0$$

的形式，其中

$$b_i=\frac{a_i}{a_0},\quad i=1,2,3,4$$

再令

$$x=u-b_1$$

又可把方程进一步化简为

$$u^4+B_2u^2+B_3u+B_4=0$$

其中

$$B_2=6(b_2-b_1^2)$$

$$B_3=4(2b_1^3-3b_1b_2+b_3)$$

$$B_4=-3b_1^4+6b_1^2b_2-4b_1b_3+b_4$$

为了要解方程 $u^4+B_2u^2+B_3u+B_4=0$，我们使用配方法。具体就是把 B_2u^2 分

成两项 λu^2 和 $B_2u^2-\lambda u^2$，同时在方程的左边加上一项$\frac{\lambda^2}{4}$再减去一项$\frac{\lambda^2}{4}$，这样我们就得到

$$u^4+\lambda u^2+\frac{\lambda^2}{4}+B_2u^2-\lambda u^2+B_3u+B_4-\frac{\lambda^2}{4}=0$$

$$\left(u^2+\frac{\lambda}{2}\right)^2-\left((\lambda-B_2)u^2-B_3u+\left(\frac{\lambda^2}{4}-B_4\right)\right)=0$$

上式中前一项已是一个平方，如果后一项也是一个平方，那么显然方程就可化为两个二次方程而解出。而后一项是完全平方的充分必要条件是括弧中的二次三项式的判别式 Δ 等于 0，也即

$$\Delta=B_3^2-4(\lambda-B_2)\left(\frac{\lambda^2}{4}-B_4\right)=0$$

或者

$$\lambda^3-B_2\lambda^2-4B_4\lambda+4(B_2B_4-B_3^2)=0$$

解上面的三次方程（这个三次方程称为四次方程的预解方程），求出 λ 以后，就像我们在上面所说的，要解的四次方程就可化为两个二次方程而解出。这种解四次方程的方法称为费拉立解法。

定义 11.6.1　称三次方程

$$\lambda^3-B_2\lambda^2-4B_4\lambda+4(B_2B_4-B_3^2)=0$$

是四次方程

$$u^4+B_2u^2+B_3u+B_4=0$$

的预解方程。

引理 11.6.1　设 u_1,u_2,u_3,u_4 是四次方程 $u^4+B_2u^2+B_3u+B_4=0$ 的根，且

$$\lambda_1=u_1u_2+u_3u_4,\quad \lambda_2=u_2u_3+u_1u_4,\quad \lambda_3=u_1u_3+u_2u_4$$

那么 $\lambda_1,\lambda_2,\lambda_3$ 恰好是 $u^4+B_2u^2+B_3u+B_4=0$ 的预解方程的三个根。

证明　由 u_1,u_2,u_3,u_4 的定义和根与系数的关系可知

$$\sigma_1=u_1+u_2+u_3+u_4=0$$

$$\sigma_2=u_1u_2+u_1u_3+u_1u_4+u_2u_3+u_2u_4+u_3u_4=B_2$$

$$\sigma_3=u_1u_2u_3+u_1u_2u_4+u_1u_3u_4+u_2u_3u_4-B_3$$

$$\sigma_4=u_1u_2u_3u_4=B_4$$

于是

$$\lambda_1+\lambda_2+\lambda_3=u_1u_2+u_1u_3+u_1u_4+u_2u_3+u_2u_4+u_3u_4=B_2$$

$$\lambda_1\lambda_2+\lambda_2\lambda_3+\lambda_1\lambda_3=$$

$$(u_1u_2+u_3u_4)(u_2u_3+u_1u_4)+(u_2u_3+u_1u_4)(u_1u_3+u_2u_4)+$$

$$(u_1u_2+u_3u_4)(u_1u_3+u_2u_4)=$$

$$u_1u_2^2u_3+u_1^2u_2u_4+u_2u_3^2u_4+u_1u_3u_4^2+u_1u_2u_3^2+u_2^2u_3u_4+$$
$$u_1^2u_3u_4+u_1u_2u_4^2+u_1^2u_2u_3+u_1u_2^2u_4+u_1u_3^2u_4+u_2u_3u_4^2=$$
$$u_1u_2u_3(u_1+u_2+u_3)+u_1u_2u_4(u_1+u_2+u_4)+$$
$$u_1u_3u_4(u_1+u_3+u_4)+u_2u_3u_4(u_2+u_3+u_4)=$$
$$-u_1u_2u_3u_4-u_1u_2u_3u_4-u_1u_2u_3u_4-u_1u_2u_3u_4=$$
$$-4u_1u_2u_3u_4=-4B_4$$
$$\lambda_1\lambda_2\lambda_3=(u_1u_2+u_3u_4)(u_2u_3+u_1u_4)(u_1u_3+u_2u_4)=$$
$$u_1^2u_2^2u_3^2+u_1^3u_2u_3u_4+u_1u_2u_3^3u_4+u_1^2u_3^2u_4^2+u_1u_2^3u_3u_4+$$
$$u_1^2u_2^2u_4^2+u_2^2u_3^2u_4^2+u_1u_2u_3u_4^2=$$
$$u_1^2u_2^2u_3^2+u_1^2u_3^2u_4^2+u_1^2u_2^2u_4^2+u_2^2u_3^2u_4^2+$$
$$u_1u_2u_3u_4(u_1^2+u_2^2+u_3^2+u_4^2)=$$
$$\sigma_3^2-2\sigma_2\sigma_4+\sigma_4(\sigma_1^2-2\sigma_2)=B_3^2-4B_2B_4$$

于是再由预解方程的根与系数的关系即得 $\lambda_1,\lambda_2,\lambda_3$ 恰好是 $u^4+B_2u^2+B_3u+B_4=0$ 的预解方程的三个根。

引理 11.6.2 四次方程 $u^4+B_2u^2+B_3u+B_4=0$ 的判别式就等于它的预解方程的判别式。

证明 设 $u^4+B_2u^2+B_3u+B_4=0$ 的判别式为 D_4，它的预解方程

$$\lambda^3-B_2\lambda^2-4B_4\lambda+4(B_2B_4-B_3^2)=0$$

的判别式为 D_3。那么由引理 11.6.1 和判别式的定义即得

$$D_3=(\lambda_1-\lambda_2)^2(\lambda_2-\lambda_3)^2(\lambda_1-\lambda_3)^2=$$
$$(u_1u_2+u_3u_4-u_2u_3-u_1u_4)^2(u_2u_3+u_1u_4-u_1u_3-u_2u_4)^2(u_1u_2+$$
$$u_3u_4-u_1u_3-u_2u_4)^2=$$
$$(u_1-u_2)^2(u_1-u_3)^2(u_1-u_4)^2(u_2-u_3)^2(u_2-u_4)^2(u_1-u_4)^2=D_4$$

引理 11.6.3 设

$$f(x)=a_0x^4+4a_1x^3+6a_2x^2+4a_3x+a_4=0,a_0>0$$
$$E=a_0a_4-4a_1a_3+3a_2^2$$
$$F=\begin{vmatrix}a_0&a_1&a_2\\a_1&a_2&a_3\\a_2&a_3&a_4\end{vmatrix}$$

那么 $f(x)$ 的判别式

$$D_4=256(E^3-27F^2)$$

证明 根据判别式的定义可知，如果把方程

$$a_0x^4+4a_1x^3+6a_2x^2+4a_3x+a_4=0,a_0>0$$

的两边都除以 a_0，那么所得的方程

$$x^4+4b_1x^3+6b_2x^2+4b_3x+b_4=0,\quad b_i=\frac{a_i}{a_0},i=1,2,3,4$$

的判别式 $\overline{D}_4=\frac{1}{a_0^6}D_4$，其中 D_4 是原方程的判别式。再令

$$x=u-b_1$$

又可把方程进一步化简为

$$u^4+B_2u^2+B_3u+B_4=0$$

这一方程的判别式和原来的方程相同。再由引理 11.5.4. 就可知道 $u^4+B_2u^2+B_3u+B_4=0$ 的判别式 $\overline{D}_4$ 就是它的预解方程 $\lambda^3-B_2\lambda^2-4B_4\lambda+4(B_2B_4-B_3^2)=0$ 的判别式 D_3，为了计算 D_3，我们在预解方程中令 $\lambda=\mu+\frac{B_2}{3}$ 就得到

$$\mu^3+p\mu+q=0$$

其中

$$p=-\left(\frac{B_2^2}{3}+4B_4\right),\quad q=-\left(\frac{2}{27}B_2^3-\frac{8}{3}B_2B_4+B_3^2\right)$$

根据上面的说明 D_3 就等于 $\mu^3+p\mu+q=0$ 的判别式 $\overline{D}_3$。

利用

$$B_2=6(b_2-b_1^2)$$
$$B_3=4(2b_1^3-3b_1b_2+b_3)$$
$$B_4=-3b_1^4+6b_1^2b_2-4b_1b_3+b_4$$

和直接计算即可得出

$$\frac{q^2}{4}+\frac{p^3}{27}=\frac{64}{a_0^6}\left(F^2-\frac{1}{27}E^3\right)$$

再由引理 11.6.1 就得出

$$D_4=a_0^6\overline{D}_4=a_0^6\overline{D}_3=-108a_0^6\left(\frac{q^2}{4}+\frac{p^3}{27}\right)=256(E^3-27F^2)$$

由定理 10.3.6(3) 和引理 11.6.3 即得出：

定理 11.6.1 设

$$f(x)=a_0x^4+4a_1x^3+6a_2x^2+4a_3x+a_4=0,a_0>0$$
$$E=a_0a_4-4a_1a_3+3a_2^2$$
$$F=\begin{vmatrix}a_0&a_1&a_2\\a_1&a_2&a_3\\a_2&a_3&a_4\end{vmatrix}$$
$$D=E^3-27F^2$$

那么

当 $D<0$ 时，方程 $f(x)=0$ 有两个不同的实根和一对共轭复根；

当 $D=0$ 时，方程 $f(x)=0$ 有重根；

当 $D>0$ 时，方程 $f(x)=0$ 有四个不同的实根或两对共轭复根。

定理 11.6.1 虽然给出了四次函数零点的某种判据，但是美中不足的是在 $D>0$ 时包含了两种可能的结论，所以并未完全解决四次函数零点的判别问题。因此为得出能完全判别的判据，还需要继续进行深入研究。

定义 11.6.2 设

$$f(x)=a_0x^4+4a_1x^3+6a_2x^2+4a_3x+a_4=0,a_0>0$$

定义

$$A_2=a_0a_2-a_1^2$$

$$A_3=2a_1^3-3a_0a_1a_2+a_0^2a_3$$

$$A_4=-3a_1^4+6a_0a_1^2a_2-4a_0^2a_1a_3+a_0^3a_4=a_0^3f\left(-\frac{a_1}{a_0}\right)$$

在前面，我们已经通过两次变换把方程

$$a_0x^4+4a_1x^3+6a_2x^2+4a_3x+a_4=0,a_0>0$$

化为了方程

$$u^4+B_2u^2+B_3u+B_4=0$$

为了最后把这个方程的实质性参数减少到两个，我们再做一次尺度变换，使四次项和二次项的系数相等。

令 $u=\sqrt{|B_2|}z$，则当 $B_2>0$（也即 $A_2>0$ 或 $a_0a_2>a_1^2$）时，方程 $u^4+B_2u^2+B_3u+B_4=0$ 化为

$$z^4+z^2+Az+B=0$$

其中

$$A=\frac{B_3}{|B_2|^{\frac{3}{2}}},\quad B=\frac{B_4}{B_2^2}$$

当 $B_2=0$（也即 $A_2=0$ 或 $a_0a_2=a_1^2$）时，方程 $u^4+B_2u^2+B_3u+B_4=0$ 的参数已减少到两个，成为

$$u^4+B_3u+B_4=0$$

当 $B_2<0$（也即 $A_2<0$ 或 $a_0a_2<a_1^2$）时，方程

$$u^4+B_2u^2+B_3u+B_4=0$$

化为

$$z^4-z^2+Az+B=0$$

令 D_+，D_0 和 D_- 分别表示方程 $z^4+z^2+Az+B=0$，$u^4+B_3u+B_4=0$ 和 $z^4-z^2+Az+B=0$ 的对应于定理 11.6.1 中 D 的判别量，那么由直接计算

可得：

引理 11.6.4　当 $B_2 > 0$(也即 $A_2 > 0$ 或 $a_0a_2 > a_1^2$) 时

$$D_+ = \frac{a_0^6}{6^6(a_0a_2 - a_1^2)^6}D$$

当 $B_2 = 0$(也即 $A_2 = 0$ 或 $a_0a_2 = a_1^2$) 时

$$D_0 = \frac{1}{a_0^6}D$$

当 $B_2 < 0$(也即 $A_2 < 0$ 或 $a_0a_2 < a_1^2$) 时

$$D_+ = \frac{a_0^6}{6^6(a_0a_2 - a_1^2)^6}D$$

因此今后凡是需用 D_+，D_0 和 D_- 的符号来判别方程的根的情况时，我们都可以用 D 来代替它们。

在上面的引理中，虽然 D_+ 和 D_- 在各自的定义域中形式上都等于 $\frac{a_0^6}{6^6(a_0a_2 - a_1^2)^6}D$，但是我们不能为了简便，把上述引理写成当 $B_2 \neq 0$(也即 $A_2 \neq 0$ 或 $a_0a_2 \neq a_1^2$) 时

$$D_+ = D_- = \frac{a_0^6}{6^6(a_0a_2 - a_1^2)^6}D$$

的形式，因为 D_+ 和 D_- 是两个不同的函数，且它们的定义域不相交。

以下分别对上面得出的三种标准型进行讨论。

1. $B_2 > 0$(也即 $a_0a_2 > a_1^2$)。

这时方程

$$a_0x^4 + 4a_1x^3 + 6a_2x + 4a_3x + a_4 = 0$$

化为方程

$$z^4 + z^2 + Az + B = 0$$

其对应于定理 11.6.1 中的判别式为

$$D_+ = \left(B + \frac{1}{12}\right)^3 - 27\left(\frac{B}{6} - \frac{1}{216} - \frac{A^2}{16}\right)^2$$

由 $D_+ = 0$ 得出 $B \geqslant -\frac{1}{12}$ 及

$$\frac{A^2}{16} = \frac{B}{6} - \frac{1}{216} \pm \sqrt{\frac{1}{27}\left(B + \frac{1}{12}\right)^3}$$

由恒等式

$$\frac{1}{27}\left(B + \frac{1}{12}\right)^3 - \left|\frac{B}{6} - \frac{1}{216}\right|^2 = \frac{1}{27}B\left(B - \frac{1}{4}\right)^2$$

得出

引理 11.6.5　当 $B \geqslant 0$ 时

$$\left|\frac{B}{6}-\frac{1}{216}\right| \leqslant \sqrt{\frac{1}{27}\left(B+\frac{1}{12}\right)^3}$$

当 $B \leqslant 0$ 时

$$\left|\frac{B}{6}-\frac{1}{216}\right| \geqslant \sqrt{\frac{1}{27}\left(B+\frac{1}{12}\right)^3}$$

由引理 11.6.5 可知，方程

$$\frac{A^2}{16} = \frac{B}{6}-\frac{1}{216}-\sqrt{\frac{1}{27}\left(B+\frac{1}{12}\right)^3}$$

只对应于参数平面 $B-A$ 上一个单独的点 $M_+\left(\frac{1}{4},0\right)$，而方程

$$\frac{A_2}{16} = \frac{B}{6}-\frac{1}{216}+\sqrt{\frac{1}{27}\left(B+\frac{1}{12}\right)^3}$$

有两个分支

$$A = \pm 4\sqrt{\frac{B}{6}-\frac{1}{216}+\sqrt{\frac{1}{27}\left(B+\frac{1}{12}\right)^3}}$$

由此就得出 $D_+=0$ 的图象如图11.6.1所示。

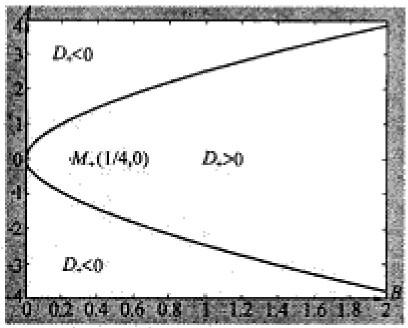


图 11.6.1 $D_+=0$ 的图象

设 $f(z)=z^4+z^2+Az+B$，那么

$$f'(z)=4z^3+2z+A=4\left(z^3+\frac{1}{2}z+\frac{A}{4}\right)$$

因此在定理 11.5.2 中 $p=\frac{1}{2}, q=\frac{A}{4}$ 而 $\Delta=\frac{A^2}{64}+\frac{1}{216}>0$。故由知 $f'(z)$ 有唯一实根，此唯一实根对应于 $f(z)$ 的唯一极小值，即最小值。因此当 B 充分大，即 $D_+>0$ 时，$f(z)$ 处于 z 轴上方，因而无实根，现在让 B 逐渐减小，那么当 B 减小到某一临界值B_0时，$f(z)$ 就恰与 z 轴相切，这时 $D_+=0$，而 $f(z)$ 有一个二重实根和一对共轭复根。当 B 小于此临界值时，$D_+<0$，$f(z)$ 与轴有两个交点，因而 $f(z)$ 有两个不同的实根和一对共轭复根。

但是 $D_+=0$ 有两个分支，其中一个是连续分支，另一个是孤立分支 $M_+\left(\frac{1}{4},0\right)$，在此孤立分支上，方程 $z^4+z^2+Az+B=0$ 成为

$$z^4+z^2+\frac{1}{4}=\left(z^2+\frac{1}{2}\right)^2=0$$

因而在点 M_+ 有 $D_+=0$，$f(z)$ 无实根。

由上面的分析知,当 $D_+ = 0$ 且 $(B,A) \neq M_+\left(\frac{1}{4},0\right)$ 时,方程 $z^4 + z^2 + Az + B = 0$ 有一个二重实根 z_* 和一对共轭复根 $\alpha_{0*} \pm \beta_{0*}\mathrm{i}$。把他们重新记为 $w, w, \alpha + \beta\mathrm{i}, \alpha - \beta\mathrm{i}$,则由根与系数的关系可知成立以下关系式

$$w + \alpha = 0$$

$$w^2 + 4w\alpha + \alpha^2 + \beta^2 = 1$$

$$w^2\alpha + w(\alpha^2 + \beta^2) = -\frac{A}{2}$$

$$w^2(\alpha^2 + \beta^2) = B$$

由此可知当 $w = 0$ 时,有 $\alpha = 0, \beta = 1; A = 0, B = 0$;当 $w \neq 0$ 时,用 w 乘 $w^2\alpha + w(\alpha^2 + \beta^2) = -\frac{A}{2}$,并将 $w(\alpha^2 + \beta^2) = B$ 代入所得的式子就得出

$$w^3\alpha + \beta = -\frac{A}{2}w$$

再将 $w + \alpha = 0$ 代入上式既得

$$-w^4 + B = -\frac{A}{2}w \quad 或 \quad w^4 - \frac{A}{2}w - B = 0$$

又从上面 4 式得出

$$w^2 - 4w^2 + \frac{B}{w^2} = 1 \quad 或 \quad 3w^4 + w^2 - B = 0$$

从 $w^4 - \frac{A}{2}w - B = 0$ 和 $3w^4 + w^2 - B = 0$ 两式得出

$$w^2 + \frac{3A}{2}w + 2B = 0$$

当 $D_+ = 0$ 且 $(B,A) \neq M_+\left(\frac{1}{4},0\right)$ 时

$$\frac{A^2}{16} = \frac{B}{6} - \frac{1}{216} + \sqrt{\frac{1}{27}\left(B + \frac{1}{12}\right)^3}, B \geqslant 0$$

或

$$\frac{9}{4}A^2 = 6B - \frac{1}{6} + \sqrt{\frac{1}{48}\left(B + \frac{1}{12}\right)^3}, B \geqslant 0$$

由此通过直接计算易于得出:

引理 11.6.6 当 $D_+ = 0$ 且 $(B,A) \neq M_+\left(\frac{1}{4},0\right)$ 时,方程 $w^2 + \frac{3A}{2}w + 2B = 0$ 的判别式

$$\Delta_2 = \frac{9}{4}A^2 - 8B \geqslant 0$$

因此方程 $w^2 + \frac{3A}{2}w + 2B = 0$ 一定存在两个实根

$$w_{1+}=\frac{-\frac{3A}{2}-\sqrt{\frac{9}{4}A^2-8B}}{2},w_{2+}=\frac{-\frac{3A}{2}+\sqrt{\frac{9}{4}A^2-8B}}{2}$$

而且通过直接计算可知当 $A>0$ 时，$z_+=w_{2+}$；当 $A=0$ 时，$z_+=0$；当 $A<0$ 时，$z_+=w_{1+}$。有

$$\alpha_{0+}=-z_+,\quad \beta_{0+}=\sqrt{1+2z_+^2}$$

通过以上讨论，我们可以得出：

引理 11.6.7 当 $a_0a_2>a_1^2$ 时

(1) 如果 $D>0$ 或者 $D=0,(B,A)=M_+\left(\frac{1}{4},0\right)$，那么方程 $z^4+z^2+Az+B=0$ 不存在任何实根；

(2) 如果 $D=0$，且 $(B,A)\neq M_+\left(\frac{1}{4},0\right)$，那么方程 $z^4+z^2+Az+B=0$ 有一个二重实根 z_+ 和一对共轭复根 $\alpha_{0+}\pm\beta_{0+}\mathrm{i}$，其中当 $A>0$ 时，$z_+=w_{2+}$；当 $A=0$ 时，$z_+=0$；当 $A<0$ 时，$z_+=w_{1+}$；有

$$\alpha_{0+}=-z_+,\quad \beta_{0+}=\sqrt{1+2z_+^2}$$

(3) 如果 $D<0$，那么方程 $z^4+z^2+Az+B=0$ 有两个不同的实根和一对共轭复根。

2. $B_2=0$（也即 $a_0a_2=a_1^2$）。

这时方程 $a_0x^4+4a_1x^3+6a_2x+4a_3x+a_4=0$ 化为方程

$$u^4+B_3u+B_4=0$$

令 $f(u)=u^4+B_3u+B_4$，那么 $f'(u)=4u^3+B_3$，因而 $f(u)$ 在 $u=-\sqrt[3]{\frac{B_3}{4}}$ 处取得唯一的极小值即最小值

$$f_{\min}=B_4-\frac{3}{4}B_3\sqrt[3]{\frac{B_3}{4}}$$

因此在 $f_{\min}>0$，即 $D_0>0$ 时，方程 $u^4+B_3u+B_4=0$ 无实根，从而方程 $a_0x^4+4a_1x^3+6a_2x+4a_3x+a_4=0$ 也无实根。当 $f_{\min}<0$，即 $D_0<0$ 时，方程 $u^4+B_3u+B_4=0$ 有两个不相等的实根和一对共轭复根。从而方程 $a_0x^4+4a_1x^3+6a_2x+4a_3x+a_4=0$ 也有两个不相等的实根和一对共轭复根。

当 $D_0=0$，且 $B_3\neq0$ 时

$$u^4+B_3u+B_4=\left(u+\sqrt[3]{\frac{B_3}{4}}\right)^2\left(u^2-2\sqrt[3]{\frac{B_3}{4}}u+3\sqrt[3]{\frac{B_3^2}{16}}\right)$$

因此当 $D_0=0$，且 $B_3\neq0$ 时，方程 $u^4+B_3u+B_4=0$ 有一个二重实根 u_{20} 和一对共轭复根 $\alpha_{00}\pm\beta_{00}\mathrm{i}$，其中 $u_{20}=-\sqrt[3]{\frac{B_3}{4}},\alpha_{00}=-u_{20},\beta_{00}=-\sqrt{2}u_{20}$。

当 $D_0=0$，且 $B_3=0$ 时，或者 $D_0=0, A_3=B_3=0$ 时，方程 $u^4+B_3u+B_4=0$ 有一个四重实根 $u_{40}=0$（图 11.6.2）。

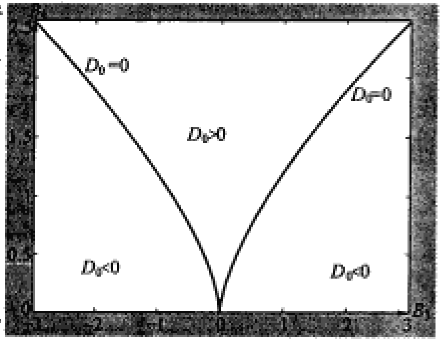


图 11.6.2　$D_0=0$ 的图象

通过以上讨论，我们可以得出：

引理 11.6.8　当 $a_0a_2=a_1^2$ 时

(1) 如果 $D>0$，那么方程 $u^4+B_3u+B_4=0$ 没有实根。

(2) 如果 $D=0$ 且 $B_3\neq 0$，那么方程 $u^4+B_3u+B_4=0$ 有一个二重实根 u_{20} 和一对共轭复根 $\alpha_{00}\pm\beta_{00}\mathrm{i}$，其中

$$u_{20}=-\sqrt[3]{\frac{B_3}{4}}, \alpha_{00}=-u_{20}, \beta_{00}=-\sqrt{2}u_{20}。$$

(3) 如果 $D_0=0$，且 $B_3=0$，或者等价的 $D_0=0, A_3=B_3=0$，那么方程 $u^4+B_3u+B_4=0$ 有一个四重实根 $u_{40}=0$。

(4) 如果 $D_0<0$，那么方程 $u^4+B_3u+B_4=0$ 有两个不相等的实根和一对共轭复根。

3. $B_2<0$（也即 $a_0a_2<a_1^2$）。

这时方程 $a_0x^4+4a_1x^3+6a_2x+4a_3x+a_4=0$ 化为方程

$$z^4-z^2+Az+B=0$$

其对应于定理 11.6.1 中的判别式为

$$D_-=\left(B+\frac{1}{12}\right)^3-27\left(-\frac{B}{6}-\frac{1}{216}-\frac{A^2}{16}\right)^2=$$

$$\left(B+\frac{1}{12}\right)^3-27\left(\frac{B}{6}-\frac{1}{216}+\frac{A^2}{16}\right)^2$$

由 $D_-=0$ 得出

$$\left(\frac{B}{6}-\frac{1}{216}+\frac{A^2}{16}\right)^2=\frac{1}{27}\left(B+\frac{1}{12}\right)^3$$

因此 $B\geqslant-\frac{1}{12}$，这时

$$\frac{B}{6}-\frac{1}{216}+\frac{A^2}{16}=\pm\sqrt{\frac{1}{27}\left(B+\frac{1}{12}\right)^3}$$

$$\frac{A^2}{16}=-\frac{B}{6}+\frac{1}{216}\pm\sqrt{\frac{1}{27}\left(B+\frac{1}{12}\right)^3}$$

由引理 11.6.5 知表达式

$$-\frac{B}{6}+\frac{1}{216}+\sqrt{\frac{1}{27}\left(B+\frac{1}{12}\right)^3}$$

在 $-\frac{1}{12}\leqslant B\leqslant 0$ 上和在 $B\geqslant 0$ 上均有意义，即在 $B\geqslant -\frac{1}{12}$ 上有意义，因此 $D_-=0$ 的两个分支为

$$A=\pm\sqrt{-\frac{B}{6}+\frac{1}{216}+\sqrt{\frac{1}{27}\left(B+\frac{1}{12}\right)^3}},B\geqslant -\frac{1}{12}$$

而表达式

$$-\frac{B}{6}+\frac{1}{216}-\sqrt{\frac{1}{27}\left(B+\frac{1}{12}\right)^3}$$

只在 $-\frac{1}{12}\leqslant B\leqslant 0$ 上有意义，因此 $D_-=0$ 的另两个分支为

$$A=\pm\sqrt{-\frac{B}{6}+\frac{1}{216}-\sqrt{\frac{1}{27}\left(B+\frac{1}{12}\right)^3}},-\frac{1}{12}\leqslant B\leqslant 0$$

用 Matlab 作图后可知 $D_-=0$ 是如图 11.6.3 所示的"燕尾"形图形。

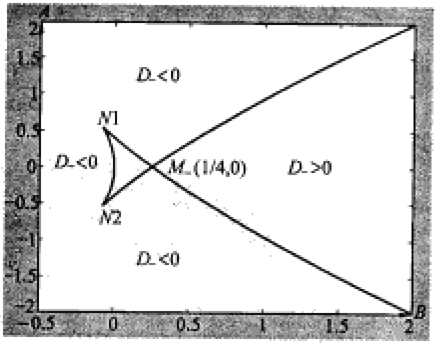


图 11.6.3　$D_-=0$ 的图象

此"燕尾"图形把整个参数平面 $B-A$ 分为三个互不连通的部分。可以证明，对应于方程 $z^4-z^2+Az+B=0$ 的无实根，有两个不同的实根，有四个不同的实根的参数区域都是 $B-A$ 平面上的开的单连通区域。因此通过在这三个单连通区域中取特殊的点或数值计算的方法，就可以确定这三个单连通区域所对应的方程 $z^4-z^2+Az+B=0$ 的情况。结果是：

当 $D_->0,B>\frac{1}{4}$ 时，方程 $z^4-z^2+Az+B=0$ 无实根；

当 $D_-<0$ 时，方程 $z^4-z^2+Az+B=0$ 有两个不相等的实根；

当 $D_->0,B<\frac{1}{4}$ 时，方程 $z^4-z^2+Az+B=0$ 有四个不相等的实根；

当 $D_-=0$，$(B,A)\neq M_-\left(\frac{1}{4},0\right)$ 或 $N_1\left(-\frac{1}{12},\frac{2\sqrt{6}}{9}\right)$ 或 $N_2\left(-\frac{1}{12},-\frac{2\sqrt{6}}{9}\right)$ 时，方程 $z^4-z^2+Az+B=0$ 有一个二重实根和一对共轭复根或者有一个二重实根和两个单的实根。由于从区域 $D_->0,B>\frac{1}{4}$ 过渡到区

域 $D_- < 0$ 时,方程 $z^4 - z^2 + Az + B = 0$ 的实根从 0 过渡到 2,因此在 $D_- = 0$, $B < \frac{1}{4}$ 时,方程 $z^4 - z^2 + Az + B = 0$ 有一个二重实根和两个单的实根。

仿照 1. 中对方程 $w^2 + \frac{3A}{2}w + 2B = 0$ 的推导可证:无论方程 $z^4 - z^2 + Az + B = 0$ 有一个二重实根 z_- 和一对共轭复根 $\alpha_{0-} \pm \beta_{0-}\mathrm{i}$ 或者有一个二重实根 z_- 和两个单的实根 z_{3-}, z_{4-},其二重实根 z_- 都必须满足方程 $w^2 - \frac{3A}{2}w - 2B = 0$。同时仿照引理 11.6.6 的证明可证:

引理 11.6.9 当 $D_- = 0$ 时,方程 $w^2 - \frac{3A}{2}w - 2B = 0$ 的判别式

$$\Delta_2 = \frac{9}{4}A^2 + 8B \geqslant 0$$

因此方程 $w^2 - \frac{3A}{2}w - 2B = 0$ 一定存在两个不同的实根

$$w_{1-} = \frac{\frac{3A}{2} - \sqrt{\frac{9A^2}{4} + 8B}}{2}, w_{2-} = \frac{\frac{3A}{2} + \sqrt{\frac{9A^2}{4} + 8B}}{2}$$

而且通过直接计算可知当 $B < \frac{1}{4}$ 时,如果 $A > 0$,那么 $z_- = w_{2-}$;如果 $A = 0$,那么 $z_- = 0$;如果 $A < 0$,那么 $z_- = w_{1-}$;有

$$z_{3-} = -z_- - \sqrt{1 - 2z_-^2}, \quad z_{4-} = -z_- + \sqrt{1 - 2z_-^2}$$

当 $B > \frac{1}{4}$ 时(注意这时 $A \neq 0$),如果 $A > 0$,那么 $z_- = w_{1-}$;如果 $A < 0$,那么 $z_- = w_{2-}, \alpha_{0-} = -z_-, \beta_{0-} = -\sqrt{1 + 2z_-^2}$。

当 $D_- = 0, (B, A) = M_-\left(\frac{1}{4}, 0\right)$ 时,方程 $z^4 - z^2 + Az + B = 0$ 成为

$$\left(z^2 - \frac{1}{2}\right)^2 = 0$$

这时,它有两个二重实根 $z_{21} = \frac{\sqrt{2}}{2}$ 和 $z_{22} = -\frac{\sqrt{2}}{2}$。

当 $D_- = 0, (B, A) = N_1\left(-\frac{1}{12}, \frac{2\sqrt{6}}{9}\right)$ 时,方程 $z^4 - z^2 + Az + B = 0$ 有一个三重实根 $z_{31} = \frac{\sqrt{6}}{6}$ 和一个单实根 $z_{21} = -3z_{31} = -\frac{\sqrt{6}}{2}$。

当 $D_- = 0, (B, A) = N_2\left(-\frac{1}{12}, -\frac{2\sqrt{6}}{9}\right)$ 时,方程 $z^4 - z^2 + Az + B = 0$ 有一个三重实根 $z_{32} = -\frac{\sqrt{6}}{6}$ 和一个单实根 $z_{22} = -3z_{32} = \frac{\sqrt{6}}{2}$。

总结以上讨论,我们得到:

引理 11.6.10 当 $a_0a_2 < a_1^2$ 时

(1) 如果 $D > 0, B > \frac{1}{4}$,那么方程 $z^4 - z^2 + Az + B = 0$ 不存在任何实根。

(2)(i) 如果 $D = 0, B > \frac{1}{4}$,那么方程 $z^4 - z^2 + Az + B = 0$ 有一个二重实根 z_- 和一对共轭复根 $\alpha_{0-} \pm \beta_{0-}\mathrm{i}$,并且如果 $A > 0$,那么 $z_- = w_{1-}$,如果 $A < 0$,那么

$$z_- = w_{2-}$$

$$\alpha_{0-} = -z_-, \quad \beta_{0-} = \sqrt{1 + 2z_-^2}$$

其中 $$w_{1-} = \frac{\frac{3A}{2} - \sqrt{\frac{9A^2}{4} + 8B}}{2}, w_{2-} = \frac{\frac{3A}{2} + \sqrt{\frac{9A^2}{4} + 8B}}{2}$$

(ii) 如果 $D = 0, B < \frac{1}{4}$,那么方程 $z^4 - z^2 + Az + B = 0$ 有一个二重实根 z_- 和两个单的实根 z_{3-} 和 z_{4-},并且如果 $A > 0$,那么 $z_- = w_{2-}$,如果 $A = 0$,那么 $z_- = 0$,如果 $A < 0$,那么

$$z_- = w_{1-}$$

$$z_{3-} = -z_- - \sqrt{1 - 2z_-^2}, \quad z_{4-} = -z_- + \sqrt{1 - 2z_-^2}$$

其中 w_{1-} 和 w_{2-} 的含义和(i)中一样。

(iii) 如果 $D = 0, (B, A) = M_-\left(\frac{1}{4}, 0\right)$,那么方程 $z^4 - z^2 + Az + B = 0$ 成为有两个二重实根 $z_{21} = \frac{\sqrt{2}}{2}$ 和 $z_{22} = -\frac{\sqrt{2}}{2}$。

(iv) 如果 $D = 0, (B, A) = N_1\left(-\frac{1}{12}, \frac{2\sqrt{6}}{9}\right)$,那么方程 $z^4 - z^2 + Az + B = 0$ 有一个三重实根 $z_{31} = \frac{\sqrt{6}}{6}$ 和一个单实根 $z_{21} = -3z_{31} = -\frac{\sqrt{6}}{2}$。

(v) 如果 $D = 0, (B, A) = N_2\left(-\frac{1}{12}, -\frac{2\sqrt{6}}{9}\right)$,那么方程 $z^4 - z^2 + Az + B = 0$ 有一个三重实根 $z_{32} = -\frac{\sqrt{6}}{6}$ 和一个单实根 $z_{22} = -3z_{32} = \frac{\sqrt{6}}{2}$。

(3) 如果 $D > 0, B < \frac{1}{4}$,那么方程 $z^4 - z^2 + Az + B = 0$ 有四个不相等的实根。

(4) 如果 $D < 0$,那么方程 $z^4 - z^2 + Az + B = 0$ 有两个不相等的实根和一对共轭复根。

综合引理 11.6.7、引理 11.6.8、引理 11.6.10 并且把 A, B, z_+, z_- 等数量用原始参数 $a_i(i = 0,1,2,3,4)$ 表出,再通过 $u - z$ 之间和 $x - u$ 之间的换算公式,

把方程 $z^4+z^2+Az+B=0$，$u^4+B_3u+B_4=0$ 和 $z^4-z^2+Az+B=0$ 的根换算成方程 $a_0x^4+4a_1x^3+6a_2x+4a_3x+a_4=0$ 的根，我们就得到：

定理 11.6.2 四次方程 $a_0x^4+4a_1x^3+6a_2x+4a_3x+a_4=0$ 的实根数目和重数由以下判据给出：

1. 当 $a_0a_2>a_1^2$ 时。

(1) 如果 $D>0$ 或者 $D=0$ 而 $2a_1^3-3a_0a_1a_2+a_0^2a_3=0$，并且 $a_0^3f\left(-\frac{a_1}{a_0}\right)=9(a_0a_2-a_1^2)^2$，那么方程 $a_0x^4+4a_1x^3+6a_2x+4a_3x+a_4=0$ 不存在任何实根。

(2) 如果 $D=0$，$2a_1^3-3a_0a_1a_2+a_0^2a_3=0$ 或者 $a_0^3f\left(-\frac{a_1}{a_0}\right)\neq 9(a_0a_2-a_1^2)^2$，那么方程 $a_0x^4+4a_1x^3+6a_2x+4a_3x+a_4=0$ 存在一个二重实根 x_+ 和一对共轭复根 $\alpha_+\pm\beta_+\mathrm{i}$，其中

$$x_+=\frac{\sqrt{6|A_2|}z_+-a_1}{a_0}$$

$$\alpha_+=\frac{-\sqrt{6|A_2|}z_+-a_1}{a_0},\beta_+=\frac{\sqrt{6|A_2|}z_+}{a_0}\beta_{0+},\beta_{0+}=\sqrt{1+2z_+^2}$$

当 $2a_1^3-3a_0a_1a_2+a_0^2a_3>0$ 时

$$z_+=\frac{-\sqrt{6}A_3+\sqrt{6A_3^2-8|A_2|A_4}}{12|A_2|^{\frac{3}{2}}}$$

当 $2a_1^3-3a_0a_1a_2+a_0^2a_3=0$ 时

$$z_+=0$$

当 $2a_1^3-3a_0a_1a_2+a_0^2a_3<0$ 时

$$z_+=\frac{-\sqrt{6}A_3-\sqrt{6A_3^2-8|A_2|A_4}}{12|A_2|^{\frac{3}{2}}}$$

(3) 如果 $D<0$，那么方程 $a_0x^4+4a_1x^3+6a_2x+4a_3x+a_4=0$ 有两个不同的实根和一对共轭复根。

2. 当 $a_0a_2=a_1^2$ 时。

(1) 如果 $D>0$，那么方程 $a_0x^4+4a_1x^3+6a_2x+4a_3x+a_4=0$ 不存在任何实根。

(2)(i) 如果 $D=0$，并且 $2a_1^3-3a_0a_1a_2+a_0^2a_3\neq 0$，那么方程 $a_0x^4+4a_1x^3+6a_2x+4a_3x+a_4=0$ 有一个二重实根 x_0 和一对共轭复根 $\alpha_0\pm\beta_0\mathrm{i}$，其中

$$x_0=u_{20}-b_1=-\sqrt{\frac{B_3}{4}}-b_1=-\frac{\sqrt[3]{A_3}+a_1}{a_0}$$

$$\alpha_0 = \alpha_{00} - b_1 = -u_{20} - b_1 = -\frac{\sqrt[3]{A_3} - a_1}{a_0}$$

$$\beta_0 = \beta_{00} = -\sqrt{2}u_{20} = \frac{\sqrt{2}\sqrt[3]{A_3}}{a_0}$$

(ii) 如果 $D = 0, 2a_1^3 - 3a_0a_1a_2 + a_0^2a_3 = 0$,或者等价的 $2a_1^3 - 3a_0a_1a_2 + a_0^2a_3 = 0$,并且 $a_0^3f\left(-\frac{a_1}{a_0}\right) = 9(a_0a_2 - a_1^2)^2$,那么方程 $a_0x^4 + 4a_1x^3 + 6a_2x + 4a_3x + a_4 = 0$ 有一个四重实根 $x_{40} = u_{40} - b_1 = -b_1 = -\frac{a}{a_0}$。

(3) 如果 $D < 0$,那么方程 $a_0x^4 + 4a_1x^3 + 6a_2x + 4a_3x + a_4 = 0$ 有两个不同的实根和一对共轭复根。

3. 当 $a_0a_2 < a_1^2$ 时。

(1) 如果 $D > 0$,且 $a_0^3f\left(-\frac{a_1}{a_0}\right) > 9(a_0a_2 - a_1^2)^2$,那么方程 $a_0x^4 + 4a_1x^3 + 6a_2x + 4a_3x + a_4 = 0$ 不存在任何实根。

(2)(i) 如果 $D = 0$, 且 $a_0^3f\left(-\frac{a_1}{a_0}\right) > 9(a_0a_2 - a_1^2)^2$, 那么方程 $a_0x^4 + 4a_1x^3 + 6a_2x + 4a_3x + a_4 = 0$ 有一个二重的实根 x_- 和一对共轭复根 $\alpha_- \pm \beta_-\mathrm{i}$,其中

$$x_- = \frac{\sqrt{6|A_2|}z_- - a_1}{a_0}$$

$$\alpha_- = \frac{-\sqrt{6|A_2|}z_- - a_1}{a_0}, \beta_- = \frac{\sqrt{6|A_2|}z_-}{a_0}\beta_{0-}, \beta_{0-} = \sqrt{1 + 2z_-^2}$$

当 $2a_1^3 - 3a_0a_1a_2 + a_0^2a_3 > 0$ 时

$$z_- = \frac{-\sqrt{6}A_3 + \sqrt{6A_3^2 - 8|A_2|A_4}}{12|A_2|^{\frac{3}{2}}}$$

当 $2a_1^3 - 3a_0a_1a_2 + a_0^2a_3 < 0$ 时

$$z_- = \frac{-\sqrt{6}A_3 - \sqrt{6A_3^2 - 8|A_2|A_4}}{12|A_2|^{\frac{3}{2}}}$$

(注意:如果 $D = 0$,且 $a_0^3f\left(-\frac{a_1}{a_0}\right) > 9(a_0a_2 - a_1^2)^2$,那么 $2a_1^3 - 3a_0a_1a_2 + a_0^2a_3$ 不可能等于 0)

(ii) 如果 $D = 0$,并且 $a_0^3f\left(-\frac{a_1}{a_0}\right) = 9(a_0a_2 - a_1^2)^2$,或者 $2a_1^3 - 3a_0a_1a_2 + a_0^2a_3 = 0$ 并且 $a_0^3f\left(-\frac{a_1}{a_0}\right) = 9(a_0a_2 - a_1^2)^2$,那么方程 $a_0x^4 + 4a_1x^3 + 6a_2x +$

$4a_3x + a_4' = 0$ 有两个二重实根 x_{21} 和 x_{22}，其中

$$x_{21} = \frac{-a_1 - \sqrt{3|A_2|}}{a_0}, x_{22} = \frac{-a_1 + \sqrt{3|A_2|}}{a_0}$$

(iii) 如果 $D = 0$，并且 $-3(a_0a_2 - a_1^2)^2 < a_0^3 f\left(-\frac{a_1}{a_0}\right) < 9(a_0a_2 - a_1^2)^2$，那么方程 $a_0x^4 + 4a_1x^3 + 6a_2x + 4a_3x + a_4 = 0$ 有一个二重的实根 x_- 和两个不同的单的实根 x_3, x_4，其中

$$x_- = \frac{\sqrt{6|A_2|}z_- - a_1}{a_0}, x_3 = \frac{\sqrt{6|A_2|}z_3 - a_1}{a_0}, x_4 = \frac{\sqrt{6|A_2|}z_4 - a_1}{a_0}$$

当 $2a_1^3 - 3a_0a_1a_2 + a_0^2a_3 > 0$ 时，$z_- = w_{2-}$；

当 $2a_1^3 - 3a_0a_1a_2 + a_0^2a_3 = 0$ 时，$z_- = 0$；

当 $2a_1^3 - 3a_0a_1a_2 + a_0^2a_3 < 0$ 时，$z_- = w_{1-}$。

$$z_{3-} = -z_- - \sqrt{1 - 2z_-^2}, \quad z_{4-} = -z_- + \sqrt{1 - 2z_-^2}$$

$$w_{1-} = \frac{\sqrt{6}A_3 - \sqrt{6A_3^2 + 8|A_2|A_4}}{12|A_2|^{\frac{3}{2}}}, w_{2-} = \frac{\sqrt{6}A_3 + \sqrt{6A_3^2 + 8|A_2|A_4}}{12|A_2|^{\frac{3}{2}}}$$

(iv) 如果 $D = 0$，并且 $-3(a_0a_2 - a_1^2)^2 = a_0^3 f\left(-\frac{a_1}{a_0}\right)$，那么方程 $a_0x^4 + 4a_1x^3 + 6a_2x + 4a_3x + a_4 = 0$ 有一个三重的实根 x_3 和一个单的实根 x_4。

当 $2a_1^3 - 3a_0a_1a_2 + a_0^2a_3 > 0$ 时

$$x_3 = \frac{-a_1 + \sqrt{|A_2|}}{a_0}, x_4 = \frac{-a_1 - 3\sqrt{|A_2|}}{a_0}$$

当 $2a_1^3 - 3a_0a_1a_2 + a_0^2a_3 < 0$ 时

$$x_3 = \frac{-a_1 - \sqrt{|A_2|}}{a_0}, x_4 = \frac{-a_1 + 3\sqrt{|A_2|}}{a_0}$$

(3) 如果 $D < 0$，那么方程 $a_0x^4 + 4a_1x^3 + 6a_2x + 4a_3x + a_4 = 0$ 有两个不同的实根和一对共轭复根。

定理 11.6.3 四次函数 $f(x) = a_0x^4 + 4a_1x^3 + 6a_2x + 4a_3x + a_4, a_0 > 0$ 是正定的充分必要条件是下列三组条件之一成立：

(1) $a_0a_2 > a_1^2$，并且

(i) $D > 0$ 或者

(ii) $D = 0$，但是 $2a_1^3 - 3a_0a_1a_2 + a_0^2a_3 = 0$，并且 $a_0^3 f\left(-\frac{a_1}{a_0}\right) = 9(a_0a_2 - a_1^2)^2$。

(2) $a_0a_2 = a_1^2, D > 0$。

(3) $a_0a_2 < a_1^2, D > 0$，并且 $a_0^3 f\left(-\frac{a_1}{a_0}\right) > 9(a_0a_2 - a_1^2)^2$。

习题 11.6

1. 判断下列方程的根的状态,并解出这些方程,再与你的判断相对照

(1) $x^4 - 2x^3 + 2x^2 + 4x - 8 = 0$

(2) $x^4 + 2x^3 - 2x^2 + 6x - 15 = 0$

(3) $x^4 - x^3 - x^2 + 2x - 2 = 0$

(4) $x^4 - 4x^3 + 3x^2 + 2x - 1 = 0$

(5) $x^4 - 3x^3 + x^2 + 4x - 6 = 0$

(6) $x^4 - 6x^3 + 6x^2 + 27x - 56 = 0$

(7) $x^4 - 2x^3 + 4x^2 - 2x + 3 = 0$

(8) $x^4 - x^3 - 3x^2 + 5x - 10 = 0$

(9) $x^4 + 2x^3 + 8x^2 + 2x + 7 = 0$

(10) $x^4 + 6x^3 + 6x^2 - 8 = 0$

(11) $x^4 - 6x^3 + 10x^2 - 2x - 3 = 0$

(12) $x^4 - 2x^3 + 4x^2 + 2x - 5 = 0$

(13) $x^4 - x^3 - 3x^2 + x + 1 = 0$

(14) $x^4 - x^3 - 4x^2 + 4x + 1 = 0$

第十二章 几个著名的数的无理性和超越性

12.1 勒让德多项式和它的性质

为了要讲什么是勒让德多项式,我们先复习一下乘积的求导公式

$$(uv)' = u'v + uv'$$

这公式又和分部积分公式有着密切的联系,从上面的式子我们又得到

$$uv' = (uv)' - u'v$$

再对上式两边积分,就得到分部积分公式

$$\int uv'\,\mathrm{d}x = uv - \int u'v\,\mathrm{d}x$$

或定积分的分部积分公式

$$\int_a^b uv'\,\mathrm{d}x = uv\,\Big|_a^b - \int_a^b u'v\,\mathrm{d}x$$

现在让我们来考虑乘积的求导公式和分部积分公式的推广问题。首先考虑乘积的求导公式的推广。也就是考虑是否能有一个用来表出$(uv)^{(n)}$的公式。为此,我们先看看对$n = 2,3$会得到什么结果,由直接计算即可得出

$$(uv)'' = u''v + 2u'v' + uv''$$

$$(uv)^{(3)} = u^{(3)}v + 3u''v' + 3u'v'' + uv^{(3)}$$

这些式子显然让我们想起二项式的展开式

$$(u+v)^2 = u^2 + 2uv + v^2$$

$$(u+v)^3 = u^3 + 3u^2v + 3uv^2 + v^3$$

$$\vdots$$

$$(u+v)^n = \sum_{k=0}^{n} C_n^k u^{n-k} v^k$$

由于它们之间的类似性,因此,由上面展开式中最后那个一般的公式很容易使人猜想对乘积求导,在一般情况下应有

$$(uv)^{(n)} = \sum_{k=0}^{n} C_n^k u^{(n-k)} v^{(k)}$$

莱布尼兹(Leibniz, Gottfried Wilhelm, 1646—1716),德国自然科学家、数学家、哲学家.生于莱比锡,卒于汉诺威.

定理 12.1.1(莱布尼兹公式) $(uv)^{(n)} = \sum_{k=0}^{n} C_n^k u^{(n-k)} v^{(k)}$。

证明 对 $n = 1,2,3$,我们已验证过这一公式成立。

现在假设这公式对于自然数 n 成立,也就是假设式子

$$(uv)^{(n)} = \sum_{k=0}^{n} C_n^k u^{(n-k)} v^{(k)}$$

成立,那么对上式两边求导就得到

$$\begin{aligned}(uv)^{(n+1)} = {} & \sum_{k=0}^{n} C_n^k u^{(n-k+1)} v^{(k)} + C_n^k u^{(n-k)} v^{(k+1)} = \\ & u^{(n+1)} v + u^{(n)} v' + C_n^1 u^{(n)} v' + C_n^1 u^{(n-1)} v'' + \cdots + \\ & C_n^{k-1} u^{(n-k+2)} v^{(k-1)} + C_n^{k-1} u^{(n-k+1)} v^{(k)} + \\ & C_n^k u^{(n-k+1)} v^{(k)} + C_n^k u^{(n-k)} v^{(k+1)} + \cdots + \\ & C_n^{n-1} u'' v^{(n-1)} + u' v^{(n)} + u v^{(n+1)} = \\ & u^{(n+1)} v + (1 + C_n^1) u^{(n)} v' + \cdots + \\ & (C_n^{k-1} + C_n^k) u^{(n-k+1)} v^{(k)} + \cdots + \\ & (C_n^{n-1} + 1) u' v^{(n)} + u v^{(n+1)} = \sum_{k=0}^{n+1} C_{n+1}^k u^{(n+1-k)} v^{(k)}\end{aligned}$$

这就说明,这一公式对自然数 $n+1$ 也成立。因而由数学归纳法就证明了公式对一切自然数 n 都成立。

例 12.1.1 求 $(x^2 \cos ax)^{(50)}$。

解 在莱布尼兹公式中令 $v = x^2, u = \cos ax$,那么

$$u^{(k)} = a^k \cos\left(ax + \frac{k\pi}{2}\right)$$

$$v' = 2x, v'' = 2, v^{(3)} = v^{(4)} = \cdots = 0$$

因此在莱布尼兹公式中除去头三项之外,其余各项都等于 0,因而

$$(x^2\cos ax)^{(50)} = x^2a^{50}\cos\left(ax+\frac{50\pi}{2}\right)+C_{50}^{1}2xa^{49}\cos\left(ax+\frac{49\pi}{2}\right)+$$

$$C_{50}^{2}2a^{48}\cos\left(ax+\frac{48\pi}{2}\right)=$$

$$a^{48}((2\,450-a^2x^2)\cos ax-100ax\sin ax)$$

现在来考虑分部积分公式的推广。

在分步积分公式

$$\int uv'\mathrm{d}x = uv-\int u'v\mathrm{d}x$$

中用 $v^{(n)}$ 代替 v' 就得到

$$\int uv^{(n)}\mathrm{d}x = uv^{(n-1)}-\int u'v^{(n-1)}\mathrm{d}x$$

再对上式中第二项进行类似的手续，并一直进行 n 次，我们就得到一般的分部积分公式。

定理 12.1.2(广义分部积分公式)

$$\int uv^{(n)}\mathrm{d}x = [uv^{(n-1)}-u'v^{(n-2)}+\cdots+(-1)^{n-1}u^{(n-1)}v]+(-1)^n\int u^{(n)}v\mathrm{d}x$$

$$\int_a^b uv^{(n)}\mathrm{d}x = [uv^{(n-1)}-u'v^{(n-2)}+\cdots+(-1)^{n-1}u^{(n-1)}v]\Big|_a^b+(-1)^n\int_a^b u^{(n)}v\mathrm{d}x$$

在上面的公式中，如果中括号中的项在 $x=a$ 处和 $x=b$ 处都变为 0，那么这个公式就将变得格外简单，这就引出勒让德多项式的概念。

定义 12.1.1 设 $P_n(x)$ 是 n 次多项式，具有性质，对任意次数低于 n 的多项式 $Q(x)$ 都有

$$\int_a^b P_n(x)Q(x)\mathrm{d}x = 0$$

则称 $P_n(x)$ 是区间 $[a,b]$ 上的 n 次勒让德多项式。

引理 12.1.1 设 $W_n(x)=\frac{\mathrm{d}^n}{\mathrm{d}x^n}(x-a)^n(x-b)^n$，$Q(x)$ 是任意次数低于 n 的多项式，那么

$$\int_a^b W_n(x)Q(x)\mathrm{d}x = 0$$

因而区间 $[a,b]$ 上的 n 次勒让德多项式是存在的。

证明 设 $R(x)=(x-a)^n(x-b)^n$，则由莱布尼兹公式易证

$$R(a)=R'(a)=\cdots=R^{(n-1)}(a)=0$$

$$R(b)=R'(b)=\cdots=R^{(n-1)}(b)=0$$

因此 $\int_a^b W_n(x)Q(x)\mathrm{d}x=0$ 对应用广义分部积分公式即可得

$$\int_a^b W_n(x)Q(x)\mathrm{d}x = \int_a^b R^{(n)}(x)Q(x)\mathrm{d}x =$$

$$(QR^{(n-1)}-Q'R^{(n-2)}+\cdots+(-1)^{n-1}Q^{(n-1)}R)\big|_a^b+$$
$$(-1)^n\int_a^b Q^{(n)}(x)R(x)\mathrm{d}x$$

由 $R(a)=R'(a)=\cdots=R^{(n-1)}(a)=0$ 和 $R(b)=R'(b)=\cdots=R^{(n-1)}(b)=0$ 可知，上式右边中括号中的各项都等于0，而由于 $Q(x)$ 是次数低于 n 的多项式，因而在上式右端的积分中 $Q^{(n)}(x)=0$，因此上式的右端等于0，这就得出 $\int_a^b W_n(x)Q(x)\mathrm{d}x=0$，因而证明了引理。

引理 12.1.2 设 $P_n(x)$ 是区间 $[a,b]$ 上的 n 次勒让德多项式，那么 $P_n(x)=c_nW_n(x)$，其中 c_n 是一个不依赖于 x 的常数。

证明 设 $R(x)=\int_a^x\int_a^x\cdots\int_a^x P_n(x)\mathrm{d}x$（共有 n 个积分号），那么易证 $R^{(n)}(x)=P_n(x)$ 且

$$R(a)=R'(a)=\cdots=R^{(n-1)}(a)=0$$

对积分 $\int_a^b P_n(x)Q(x)\mathrm{d}x=0$（其中 $Q(x)$ 是任意次数低于 n 的多项式）应用广义分部积分公式得

$$\int_a^b P_n(x)Q(x)\mathrm{d}x=\int_a^b R^{(n)}(x)Q(x)\mathrm{d}x=$$
$$(QR^{(n-1)}-Q'R^{(n-2)}+\cdots+(-1)^{n-1}Q^{(n-1)}R)\big|_a^b+$$
$$(-1)^n\int_a^b Q^{(n)}(x)R(x)\mathrm{d}x$$

按照假设有 $\int_a^b P_n(x)Q(x)\mathrm{d}x=0$，同时由于 $Q(x)$ 是次数低于 n 的多项式，因此 $Q^{(n)}(x)=0$，故 $\int_a^b Q^{(n)}(x)R(x)\mathrm{d}x=0$，这就得出

$$Q(b)R^{(n-1)}(b)-Q'(b)R^{(n-2)}(b)+\cdots+(-1)^{n-1}Q^{(n-1)}(b)R(b)=0$$

由于 $Q(x)$ 是任意次数低于 n 的多项式，故对于 $Q(x)=(x-b)^{(n-1)},(x-b)^{(n-2)},\cdots,x-b$ 上式都成立，把这些函数依次代入上式即可得

$$R(b)=R'(b)=\cdots=R^{(n-1)}(b)=0$$

由 $R(a)=R'(a)=\cdots=R^{(n-1)}(a)=0,R(b)=R'(b)=\cdots=R^{(n-1)}(b)=0$ 说明 a,b 分别是 $R(x)$ 的 n 重根，而由于 $P_n(x)$ 是 n 次多项式，因而 $R(x)$ 是 $2n$ 次多项式。因此 $R(x)$ 只可能与 $(x-a)^n(x-b)^n$ 相差一个常数 c_n，即

$$R(x)=c_n(x-a)^n(x-b)^n$$

故

$$P_n(x)=R^{(n)}(x)=c_n\frac{\mathrm{d}^n}{\mathrm{d}x^n}(x-a)^n(x-b)^n=c_nW_n(x)$$

下面我们来看一下勒让德多项式，特别是区间[0,1]上的勒让德多项式的一些性质。

引理 12.1.3 设 $P_n(x)=\frac{1}{n!}\frac{d^n}{dx^n}x^n(1-x)^n$，那么

$$\int_0^1 P_n(x)P_m(x)dx=\begin{cases}0, & m\neq n\\ \frac{1}{2n+1}, & m=n\end{cases}$$

证明 当 $m\neq n$ 时，由 $P_n(x)$ 的定义及引理 12.1.1、引理 12.1.2 及其证明即知

$$\int_0^1 P_n(x)P_m(x)dx=0$$

当 $m=n$ 时，设 $R(x)=x^n(1-x)^n$，那么

$$\int_0^1 P_n(x)P_m(x)dx=\int_0^1 P_n^2(x)dx=\frac{1}{(n!)^2}\int_0^1 R^2(x)dx=$$

$$\frac{1}{(n!)^2}((R^{(n)}R^{(n-1)}-R^{(n+1)}R^{(n-2)}+\cdots+$$

$$(-1)^{n-1}R^{(2n-1)}R)_0^1+(-1)^n\int_0^1 R^{(2n)}Rdx)=$$

$$\frac{(-1)^n}{(n!)^2}\int_0^1 R^{(2n)}Rdx$$

而由二项式的展开式有

$$R^{(2n)}=(x^n(1-x)^n)^{(2n)}=(x^n(1-C_n^1x+C_n^2x^2+\cdots+(-1)^nx^n))^{(2n)}=$$

$$(x^n-C_n^1x^{n+1}+C_n^2x^{n+2}+\cdots+(-1)^nx^{2n})^{(2n)}=(-1)^n(2n)!$$

因此

$$\int_0^1 P_n^2(x)dx=\frac{(-1)^n(-1)^n(2n)!}{(n!)^2}\int_0^1 R(x)dx=\frac{(2n)!}{(n!)^2}\int_0^1 x^n(1-x)^ndx=$$

$$\frac{(2n)!}{(n!)^2}B(n+1,n+1)=\frac{(2n)!}{(n!)^2}\frac{\Gamma(n+1)\Gamma(n+1)}{\Gamma(2n+2)}=$$

$$\frac{(2n)!}{(n!)^2}\frac{(n!)(n!)}{(2n+1)!}=\frac{1}{2n+1}$$

引理 12.1.4 设 $P_n(x)=\frac{1}{n!}\frac{d^n}{dx^n}x^n(1-x)^n$，那么

(1) $P_n(x)$ 是整系数多项式；

(2) $P_n(0)=1, P_n(1)=(-1)^n$。

证明 (1) 设 $u=(1-x)^n, v=x^n$，那么

$$u(k)=(-1)^kA_n^k(1-x)^{n-k}=(-1)^kn(n-1)\cdots(n-k+1)(1-x)^{n-k}=$$

$$(-1)^k\frac{n!}{(n-k)!}(1-x)^{n-k}$$

$$v^{(n-k)} = A_n^{n-k}x^k = n(n-1)\cdots(k+1)x^k$$

而

$$P_n(x) = \frac{(uv)^{(n)}}{n!} = \frac{1}{n!}(uv^{(n)} + C_n^1u'v^{(n-1)} + \cdots + C_n^k u^{(k)}v^{(n-k)} + \cdots + u^{(n)}v) =$$

$$\frac{1}{n!}(n!(1-x)^n + \sum_{k=1}^{n-1}(-1)^k C_n^k \frac{n!}{(n-k)} \cdot \frac{n!}{k!}(1-x)^{n-k}x^k +$$

$$(-1)^n n!x^n) = \frac{1}{n!}(n!(1-x)^n +$$

$$\sum_{k=1}^{n-1}(-1)^k C_n^k \frac{n!}{(n-k)k!} \cdot n!(1-x)^{n-k}x^k + (-1)^n n!x^n) =$$

$$\frac{1}{n!}(n!(1-x)^n + (-1)^k n!\sum_{k=1}^{n-1}(C_n^k)^2(1-x)^{n-k}x^k + (-1)^n n!x^n) =$$

$$(1-x)^n + (-1)^k\sum_{k=1}^{n-1}(C_n^k)^2(1-x)^{n-k}x^k + (-1)^n x^n$$

显然上式是一个整系数多项式的整系数线性组合，因此仍然是一个整系数多项式，这就证明了引理的第一部分。

(2) 在(1)中所得的式子中令 $x = 0$ 和 $x = 1$ 即得 $P_n(0) = 1, P_n(1) = (-1)^n$。

引理 12.1.5 设 $P_n(x) = \frac{1}{n!}\frac{d^n}{dx^n}x^n(1-x)^n$，那么

$$P_n'(0) = -(n^2+n), P_n'(1) = (-1)^n(n^2+n)$$

证明 由引理 12.1.4 的证明知

$$P_n = (1-x)^n - (C_n^1)^2(1-x)^{n-1}x + [\cdots] +$$
$$(-1)^{n-1}(C_n^{n-1})^2(1-x)x^{n-1} + (-1)^n x^n$$

其中$[\cdots]$中的项都是形如$(1-x)^i x^j$的单项式的线性组合，这里 $i+j=n, i \geqslant 2, j \geqslant 2$。因此$[\cdots]$中的式子在求导一次后，在 $x=0$ 和 $x=1$ 处的值都是 0。因而

$$P_n' = n(1-x)^{n-1}(-1) - (C_n^1)^2((n-1)(1-x)^{n-2}(-1)x + (1-x)^{n-1}) + [\cdots]' +$$
$$(-1)^{n-1}(C_n^{n-1})^2(-x^{n-1} + (n-1)(1-x)x^{n-2}) + (-1)^n nx^{n-1}$$

由上式就得出

$$P_n'(0) = -n - n^2[0+1] + 0 + (-1)^{n-1}n^2[0+0] + 0 = -(n^2+n)$$
$$P_n'(1) = 0 - n^2[0+0] + 0 + (-1)^{n-1}n^2[-1+0] + (-1)^n n =$$
$$(-1)^n(n^2+n)$$

引理 12.1.6 设 $P_n(x) = \frac{1}{n!}\frac{d^n}{dx^n}x^n(1-x)^n$，那么 $P_n = \sum_{k=0}^{n}(-1)^k C_n^k C_{n+k}^k x^k$。

证明

$$P_n(x)=\frac{d^n}{dx^n}\frac{1}{n!}x^n(1-x)^n=\frac{d^n}{dx^n}\frac{1}{n!}x^n\sum_{k=0}^{n}(-1)^k C_n^k x^k=$$

$$\frac{1}{n!}\sum_{k=0}^{n}(-1)^k C_n^k x^{n+k}=\frac{1}{n!}\sum_{k=0}^{n}(-1)^k C_n^k\frac{d^n}{dx^n}x^{n+k}=$$

$$\frac{1}{n!}\sum_{k=0}^{n}(-1)^k C_n^k P_{n+k}^n x^k=\sum_{k=0}^{n}(-1)^k C_n^k\frac{(n+k)!}{k!n!}x^k=$$

$$\sum_{k=0}^{n}(-1)^k C_n^k C_{n+k}^k x^k$$

引理 12.1.7 设 $P_n(x)=\frac{1}{n!}\frac{d^n}{dx^n}x^n(1-x)^n$,那么 $P_n(x)$ 满足关系式

$$(x-x^2)P_n''+(1-2x)P_n'+n(n+1)P_n=0$$

证明 设 $y=x^n(1-x)^n=(x-x^2)^n$,那么 $y'=n(1-2x)(x-x^2)^{n-1}$,因而

$$(x-x^2)y'=n(1-2x)y$$

在上式两边各取 $n+1$ 次导数,并利用莱布尼兹公式即得

$$(x-x^2)y^{(n+2)}+(n+1)(1-2x)y^{(n+1)}+\frac{n(n-1)}{2}(-2)y^{(n)}=$$

$$n((1-2x)y^{(n+1)}+(n+1)(-2)y^{(n)})=$$

$$n(1-2x)y^{(n+1)}-2n(n+1)y^{(n)}$$

将上式化简即得

$$(x-x^2)y^{(n+2)}+(1-2x)y^{(n+1)}+n(n+1)y^{(n)}=0$$

在上式两边都乘以$\frac{1}{n!}$ 并注意

$$P_n''=\left(\left(\frac{y}{n!}\right)^{(n)}\right)''=\frac{y^{(n+2)}}{n!},P_n'=\left(\left(\frac{y}{n!}\right)^{(n)}\right)'=\frac{y^{(n+1)}}{n!},P_n=\frac{y^{(n)}}{n!}$$

即得引理。

12.2 e的无理性

定理 12.2.1 e是无理数。

证明 从数学分析中知道

$$e=1+\frac{1}{1!}+\frac{1}{2!}+\cdots+\frac{1}{n!}+\cdots=$$

$$1+\frac{1}{1!}+\frac{1}{2!}+\cdots+\frac{1}{n!}+\frac{1}{(n+1)!}\left(1+\frac{1}{n+2}+\frac{1}{(n+2)(n+3)}+\cdots\right)$$

故

$$n!e=I_n+R_n$$

其中 $I_n = n!\left(1+\frac{1}{1!}+\frac{1}{2!}+\cdots+\frac{1}{n!}\right)$ 是整数。而

$$R_n = \frac{1}{n+1}\left(1+\frac{1}{n+2}+\frac{1}{(n+2)(n+3)}+\cdots\right)$$

当 $n \geqslant 2$ 时

$$0 < R_n < \frac{1}{n+1}\left(1+\frac{1}{n+1}+\frac{1}{(n+1)(n+2)}+\cdots\right) <$$
$$\frac{1}{n+1}\left(1+\frac{1}{1!}+\frac{1}{2!}+\cdots+\frac{1}{n!}+\cdots\right) \leqslant \frac{e}{n+1} < 1(\text{因为 } e < 3)$$

这样，如果 $e = \frac{a}{b}$ 是一个有理数，那么当 $n > b$ 时，由 $n!e = I_n + R_n$ 就得出一个等式，它的左边是整数，而右边不是整数，这显然是一个矛盾，所得的矛盾就说明，e 不可能是一个有理数。

12.3 π的无理性

引理 12.3.1 设 $J_m = \int_0^1 x^m \sin \pi x\,dx, K_m = \int_0^1 x^m \cos \pi x\,dx$，那么

$$J_{2n-1} = \frac{\pi^{2n-1} - (2n-1)(2n-1)\pi^{2n-3} + \cdots + (-1)^{n-1}(2n-1)\cdots 2\pi}{\pi^{2n}}$$

$$J_{2n} = \frac{\pi^{2n} - 2n(2n-1)\pi^{2n-2} + \cdots + 2n(2n-1)\cdots 3\pi^2 + (-1)^n \cdot 2 \cdot 2n(2n-1)\cdots 1}{\pi^{2n+1}}$$

$$K_m = -\frac{m}{\pi}J_{m-1}$$

因而 $J_m = \frac{p_m}{\pi^{m+1}}, K_m = \frac{q_m}{\pi^{m+1}}$，其中 p_m, q_m 都是次数至多为 m 的 π 的整系数多项式。

证明 首先我们有

$$J_{m+1} = \int_0^1 x^{m+1}\sin \pi x\,dx = -\frac{\cos \pi x}{\pi}x^{m+1}\Big|_0^1 + \frac{m+1}{\pi}\int_0^1 x^m \cos \pi x\,dx =$$
$$\frac{1}{\pi} + \frac{m+1}{\pi}K_m$$

$$K_{m+1} = \int_0^1 x^{m+1}\cos \pi x\,dx = \frac{\sin \pi x}{\pi}x^{m+1}\Big|_0^1 - \frac{m+1}{\pi}\int_0^1 x^m \sin \pi x\,dx = -\frac{m+1}{\pi}J_m$$

当 $m = 0$ 时

$$\int_0^1 \sin \pi x\,dx = \frac{2}{\pi}, \int_0^1 \cos \pi x\,dx = 0, p_0 = 2, q_0 = 0$$

当 $m = 1$ 时

$$\int_0^1 x\sin \pi x\mathrm{d}x = \frac{1}{\pi},\int_0^1 \cos \pi x\mathrm{d}x = -\frac{2}{\pi^2},p_1 = \pi,q_1 = -2$$

因此对自然数 $m = 0,1$ 引理成立。现在假设对小于或等于 m 的自然数，引理成立，即设

$$J_{2n-1} = \frac{1}{\pi^{2n}}\sum_{k=0}^{n-1}(-1)^k A_{2n-1}^{2k}\pi^{2n-1-2k}$$

$$J_{2n} = \frac{1}{\pi^{2n+1}}\left(\sum_{k=0}^{n-1}(-1)^k A_{2n}^{2k}\pi^{2n-2k} + (-1)^n \cdot 2 \cdot A_{2n}^{2n}\right)$$

那么

$$J_{2n+1} = \frac{1}{\pi} + \frac{2n+1}{\pi}K_{2n} = \frac{1}{\pi} + \frac{2n+1}{\pi}\left(-\frac{2n}{\pi}J_{2n-1}\right) =$$

$$\frac{1}{\pi} - \frac{(2n+1)2n}{\pi^2}\frac{1}{\pi^{2n}}\sum_{k=0}^{n-1}(-1)^k A_{2n-1}^{2k}\pi^{2n-1-2k} =$$

$$\frac{\pi^{2n+1} - (2n+1)\cdot 2n\sum_{k=0}^{n-1}(-1)^k A_{2n-1}^{2k}\pi^{2n-1-2k}}{\pi^{2n+2}} =$$

$$\frac{1}{\pi^{2n+2}}\sum_{k=0}^{n}(-1)^k A_{2n+1}^{2k}\pi^{2n+1-2k}$$

类似可证

$$J_{2n+2} = \frac{1}{\pi^{2n+3}}\left(\sum_{k=0}^{n}(-1)^k A_{2n}^{2k} + 2\pi^{2n+2-2k} + (-1)^{n+1}\cdot 2 \cdot A_{2n+2}^{2n+2}\right)$$

这就说明，J_m 的表达式对自然数 $2n+1,2n+2$ 也成立，因而由数学归纳法知这一表达式对任何自然数都成立。由一开始的证明中的分部积分我们已经证明了 $K_m = -\frac{m}{\pi}J_{m-1}$。

根据已经证明的关于 J_m,K_m 的公式即可得出 $J_m = \frac{p_m}{\pi^{m+1}},K_m = \frac{q_m}{\pi^{m+1}}$，其中 p_m,q_m 都是次数至多为 m 的 π 的整系数多项式。

引理 12.3.2 设 $\bar{p}_n(x)$ 是 x 的次数不超过 n 的整系数多项式，那么

$$\int_0^1 \bar{p}_n(x) * (\pi x)\mathrm{d}x = \frac{p_n}{\pi^{n+1}}$$

其中 $*$ 号表示 sin 或 cos。

证明 设 $\bar{p}_n(x) = a_0 + a_1x + \cdots + a_nx^n$，其中 $a_0,a_1,\cdots,a_n$ 都是整数。那么由引理 12.3.1 得知

$$\int_0^1 \bar{p}_n(x) * (\pi x)\mathrm{d}x = \int_0^1 (a_0 + a_1x + \cdots + a_nx^n) * (\pi x)\mathrm{d}x =$$

$$\left(a_0\int_0^1 + a_1\int_0^1 x + \cdots + a_n\int_0^1 x^n\right) * (\pi x)\mathrm{d}x =$$

$$\frac{a_0\tilde{p}_0}{\pi}+\frac{a_1\tilde{p}_1}{\pi^2}+\cdots+\frac{a_n\tilde{p}_n}{\pi^{n+1}}=$$

$$\frac{a_0\pi^n\tilde{p}_0+a_1\pi^{n-1}\tilde{p}_1+\cdots+a_n\tilde{p}_n}{\pi^{n+1}}=\frac{p_n}{\pi^{n+1}}$$

其中 $\tilde{p}_k$ 是 π 的次数不超过 k 的整系数多项式,因此整系数线性组合

$$p_n=a_0\pi^n\tilde{p}_0+a_1\pi^{n-1}\tilde{p}_1+\cdots+a_n\tilde{p}_n$$

也是 π 的次数不超过 k 的整系数多项式。

引理 12.3.3 设 $p(x)$ 具有性质:

(1) $p(0)=p'(0)=\cdots=p^{(n-1)}(0)=0$;

(2) $p(1)=p'(1)=\cdots=p^{(n-1)}(1)=0$;

(3) $p^{(n)}(x)$ 是整系数多项式,则

$$\int_0^1 p(x)*(\pi x)\mathrm{d}x=\frac{p_n}{\pi^{2n+1}}$$

其中 $*$ 号表示 sin 或 cos。

证明 令 $\overline{*}$ 表示 cos(当 $*$ 号表示 sin 时)或 sin(当 $*$ 号表示 cos 时)。那么由广义分部积分公式就有

$$\int_0^1 p(x)*(\pi x)\mathrm{d}x=\left(\epsilon_1\frac{p\overline{*}(\pi x)}{\pi}+\epsilon_2\frac{p'*(\pi x)}{\pi^2}+\cdots+\epsilon_n\frac{p^{(n-1)}\overline{*}^n(\pi x)}{\pi^n}\right)\Bigg|_0^1+$$

$$\frac{\epsilon_{n+1}}{\pi^n}\int_0^1 p^{(n)}(x)\overline{*}^n(\pi x)\mathrm{d}x$$

其中,$\epsilon_1,\epsilon_2,\cdots,\epsilon_n$ 表示 $+1$ 或 -1,$\overline{*}^2$ 表示 $\overline{\overline{*}}=*$,…。

由 $p(x)$ 的性质(1),(2)可知,上式的右边中括号中的项全为 0,而由性质(3)和引理 12.3.2 知

$$\int_0^1 p^{(n)}(x)\overline{*}^n(\pi x)\mathrm{d}x=\frac{\tilde{p}_n}{\pi^{n+1}}$$

其中 $\tilde{p}$ 是 π 的次数不超过 n 的整系数多项式,因而

$$\int_0^1 p(x)*(\pi x)\mathrm{d}x=\frac{\epsilon_{n+1}}{\pi^{n+1}}\tilde{p}_n=\frac{p_n}{\pi^{2n+1}}$$

其中 p_n 是 π 的次数不超过 n 的整系数多项式。

引理 12.3.4 设 $R_n(x)=\dfrac{x^n(1-x)^n}{n!}$,则

$$\int_0^1 R_n(x)\sin\pi x\mathrm{d}x=\frac{p_n}{\pi^{2n+1}}$$

其中 p_n 是 π 的次数不超过 n 的多项式。

证明 由引理 12.1.1 的证明知,$R_n(x)$ 具有引理 12.3.3 的性质(1),(2),由引理 12.1.4 知 $R_n(x)$ 具有引理 12.3.3 的性质(3),因此由引理 12.3.3 即得引

理12.3.4成立。

引理12.3.5 $\int_0^1 x^n(1-x)^n\cos\pi x\mathrm{d}x = 0$。

证明 设 $I = \int_0^1 x^n(1-x)^n\cos\pi x\mathrm{d}x$，并在此积分中令 $x = 1-y$，那么 $\mathrm{d}x = -\mathrm{d}y$，而

$$I = \int_1^0 (1-y)^n y^n \cos\pi(1-y)(-\mathrm{d}y) = -\int_0^1 y^n(1-y)^n\cos(\pi-\pi y)(-\mathrm{d}y) = -\int_0^1 y^n(1-y)^n\cos\pi y\mathrm{d}y = -I$$

由此即得出 $I = 0$。

引理12.3.6 设 $P_n(x) = \frac{1}{n!}\frac{\mathrm{d}^n}{\mathrm{d}x^n}x^n(1-x)^n$，那么$\int_0^1 P_{2n-1}(x)\sin\pi x\mathrm{d}x = 0$。

证明 易证

$$(\sin x)^{(2n-1)} = (-1)^{n-1}\cos x, (\sin x)^{(2n)} = (-1)^n\sin x$$

并注意
$$P_{2n-1}(x) = R^{(2n-1)}(x)$$

其中
$$R(x) = \frac{1}{(2n-1)!}x^{2n-1}(1-x)^{2n-1}$$

利用广义分部积分公式及 R 本身和 R 的前 $2n-2$ 阶导数在 $x=0$ 和 $x=1$ 处都为0的性质即可得

$$\int_0^1 P_{2n-1}(x)\sin\pi x\mathrm{d}x = \int_0^1 R^{(2n-1)}(x)\sin\pi x\mathrm{d}x = [R^{(2n-2)}\sin\pi x - \pi R^{(2n-3)}\cos\pi x + \cdots + (-1)^{2n-2}R(\sin\pi x)^{2n-2}]\Big|_0^1 + (-1)^{2n-1}\int_0^1 R(\sin\pi x)^{(2n-1)}\mathrm{d}x = \frac{(-1)^{2n-1}\pi^{2n-1}}{(2n-1)!}\int_0^1 x^{2n-1}(1-x)^{2n-1}\cos\pi x\mathrm{d}x = 0$$

(引理12.3.5)

定理12.3.1 π是无理数。

证明 由引理12.3.4知

$$I_n = \frac{1}{n!}\int_0^1 x^n(1-x)^n\sin\pi x = \frac{p_n}{\pi^{n+1}}$$

其中，p_n 是 π 的次数不超过 n 的多项式。显然，对于任何自然数 n 都有 $I_n > 0$。

如果π是一个有理数，则可设 $\pi = \frac{a}{b}$，其中 a, b 都是正整数。那么一方面有

$$I_n = \frac{p_n}{\pi^{n+1}} = \frac{p_n\left(\frac{a}{b}\right)}{\left(\frac{a}{b}\right)^{n+1}} = \frac{b^{n+1}p_n\left(\frac{a}{b}\right)}{a^{n+1}} = \frac{N_n}{a^{n+1}}$$

其中 N_n 是一个依赖于 n 的正整数。

另一方面又有在区间[0,1]上 $0 \leqslant x(1-x) \leqslant \frac{1}{4}$,因此有当 $n \to \infty$ 时

$$N_n = a^{n+1} I_n \leqslant \frac{a^{n+1}}{n!}\left(\frac{1}{4}\right)^n \to 0$$

这与 N_n 是正整数矛盾,所得的矛盾就说明 π 不可能是一个有理数,即 π 是无理数。

12.4 ln 2的无理性

引理 12.4.1 $\int_0^1 \frac{x^n}{1+x}\mathrm{d}x = \frac{1}{n} - \frac{1}{n-1} + \cdots + (-1)^{n-1} + (-1)^n \ln 2$。

证明 易证恒等式

$$\frac{x^n}{1+x} = x^{n-1} - x^{n-2} + \cdots + (-1)^{n-1} + \frac{(-1)^n}{1+x}$$

对上面的恒等式两边在[0,1]上积分,即得引理。

引理 12.4.2 设 $f(x)$ 是 n 次的整系数多项式,则

$$\int_0^1 \frac{f(x)}{1+x}\mathrm{d}x = \frac{b_n}{n} + \frac{b_{n-1}}{n-1} + \cdots + b_1 + b_0 \ln 2$$

证明 设 $f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n$,那么由引理 12.4.1 即得

$$\int_0^1 \frac{f(x)}{1+x}\mathrm{d}x = \int_0^1 \frac{a_0 x^n + a_1 x^{n-1} + \cdots + a_n}{1+x}\mathrm{d}x =$$

$$a_0\int_0^1 \frac{x^n}{1+x}\mathrm{d}x + a_1\int_0^1 \frac{x^{n-1}}{1+x}\mathrm{d}x + \cdots +$$

$$a_{n-1}\int_0^1 \frac{x}{1+x}\mathrm{d}x + a_n\int_0^1 \frac{1}{1+x}\mathrm{d}x =$$

$$a_0\left(\frac{1}{n} - \frac{1}{n-1} + \cdots + (-1)^{n-1} + (-1)^n \ln 2\right) +$$

$$a_1\left(\frac{1}{n-1} - \frac{1}{n-2} + \cdots + (-1)^{n-2} + (-1)^{n-1} \ln 2\right) + \cdots +$$

$$a_n \ln 2 = \frac{b_n}{n} + \frac{b_{n-1}}{n-1} + \cdots + b_1 + b_0 \ln 2$$

定理 12.4.1 ln 2 是无理数。

证明 考虑积分

$$I_n = \int_0^1 \frac{P_n(x)}{1+x}\mathrm{d}x$$

其中 $P_n(x)$ 是区间[0,1]上的勒让德多项式,即

$$P_n(x)=\frac{1}{n!}\frac{\mathrm{d}^n}{\mathrm{d}x^n}x^n(1-x)^n$$

那么由广义分部积分公式得

$$I_n=\int_0^1\frac{1}{n!}x^n(1-x)^n\frac{\mathrm{d}^n}{\mathrm{d}x^n}\frac{1}{1+x}\mathrm{d}x=\int_0^1\frac{1}{n!}x^n(1-x)^n\frac{\mathrm{d}^n}{\mathrm{d}x^n}(1+x)^{-1}\mathrm{d}x=$$

$$\int_0^1\frac{1}{n!}x^n(1-x)^n(-1)^n n!(1+x)^{-1-n}\mathrm{d}x=(-1)^n\int_0^1\frac{x^n(1-x)^n}{(1+x)^{n+1}}\mathrm{d}x$$

由上式看出 $|I_n|>0$。

由引理 12.1.4 知 $P_n(x)$ 是整系数多项式，再由引理 12.4.2 就得出

$$I_n=\frac{b_n}{n}+\frac{b_{n-1}}{n-1}+\cdots+b_1+b_0\ln 2$$

如果 $\ln 2$ 是有理数，那么 $\ln 2=\frac{a}{b}$，其中 a,b 都是正整数。而

$$I_n=\frac{b_n}{n}+\frac{b_{n-1}}{n-1}+\cdots+b_1+b_0\frac{a}{b}=\frac{N_n}{bd_n}$$

其中 N_n 是一个不等于0的整数，$d_n=[1,2,\cdots,n]$ 是前 n 个自然数 $1,2,\cdots,n$ 的最小公倍数。因此

$$|N_n|=|bd_nI_n|=bd_n\int_0^1\left(\frac{x(1-x)}{1+x}\right)^n\frac{\mathrm{d}x}{1+x}$$

令
$$f(x)=\frac{x(1-x)}{1+x}=2-x-\frac{2}{1+x}$$

则
$$f'(x)=-1+\frac{2}{(1+x)^2}=\frac{2-(1-x)^2}{(1+x)^2}$$

由此得出，当 $x\leqslant\sqrt{2}-1$ 时，$f'(x)\geqslant 0$，当 $x>\sqrt{2}-1$ 时，$f'(x)<0$。故 $f(x)$ 在 $x=\sqrt{2}-1$ 处取得极大值 $f(\sqrt{2}-1)=3-2\sqrt{2}$。又 $f(0)=f(1)=0<3-2\sqrt{2}$，故 $f(x)$ 在 $[0,1]$ 上的最大值即为 $f(\sqrt{2}-1)=3-2\sqrt{2}$。又已知对一切自然数成立 $d_n<3^n$（见第三章定理 3.8.14），故

$$|N_n|=bd_n\int_0^1\left(\frac{x(1-x)}{1+x}\right)^n\frac{\mathrm{d}x}{1+x}<b\cdot 3^n\int_0^1(3-2\sqrt{2})^n 1\mathrm{d}x\leqslant$$
$$b(3(3-2\sqrt{2}))^n$$

由于 $0<3(3-2\sqrt{2})<1$，故当 $n\to\infty$ 时，$b(3(3-2\sqrt{2}))^n\to 0$。这与 $|N_n|$ 是不等于 0 的整数相矛盾。所得的矛盾就说明 $\ln 2$ 不可能是有理数，因而是无理数。

12.5　ζ(2) 的无理性

$1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}+\cdots$ 是一个很有名的级数，称为调和级数，用很初等的方法即可证明这一级数是发散的。在下一章，我们还会遇到它。除了调和级

数，数学家们还考虑了更一般的类似的级数，称为广义调和级数，其形式如下

$$1+\frac{1}{2^s}+\frac{1}{3^s}+\cdots+\frac{1}{n^s}+\cdots$$

利用数学分析中的知识可以证明，广义调和级数当 $s>1$ 时是收敛的，因此这一级数的和是 s 的函数。

定义 12.5.1 记 $\zeta(s)=1+\frac{1}{2^s}+\frac{1}{3^s}+\cdots+\frac{1}{n^s}+\cdots$。函数 $\zeta(s)$ 对一切实数 $s>1$ 有意义。

实际上还可以证明，函数 $\zeta(s)$ 可以延拓到复平面中的半平面 $\mathrm{Re}(s)>1$ 上去，并且在此半平面上是 s 的解析函数。但是我们不准备搞的这么复杂。读者只要知道它对一切实数 $s>1$ 有意义就够了。

这一节的主要目的是证明 $\zeta(2)$ 的无理性，我们要做的第一件事是给出 $\zeta(2)$ 的一些表示式以及它同著名的 π 之间的关系。

引理 12.5.1 $\zeta(2)=-\int_0^1\frac{\ln x}{1-x}\mathrm{d}x$。

证明 在积分 $\int_0^1\frac{\ln x}{1-x}\mathrm{d}x$ 中令 $1-x=y$，那么 $\mathrm{d}x=-\mathrm{d}y$，有

$$\int_0^1\frac{\ln x}{1-x}\mathrm{d}x=\int_1^0\frac{\ln(1-y)}{y}(-\mathrm{d}y)=\int_0^1\frac{\ln(1-y)}{y}\mathrm{d}y=$$

$$\int_0^1\frac{1}{y}\left(-y-\frac{y^2}{2}-\frac{y^3}{3}-\cdots\right)\mathrm{d}y=-\int_0^1\left(1+\frac{y}{2}+\frac{y^2}{3}+\cdots\right)\mathrm{d}y=$$

$$-\left(y+\frac{y^2}{2^2}+\frac{y^3}{3^2}+\cdots\right)\Big|_0^1=-\left(1+\frac{1}{2^2}+\frac{1}{3^2}+\cdots\right)=-\zeta(2)$$

引理 12.5.2 $\zeta(2)=\int_0^1\int_0^1\frac{\mathrm{d}x\mathrm{d}y}{1-xy}$。

证明 设 $0\leqslant x<1, 0\leqslant y<1$，那么 $0\leqslant xy<1$，因而成立展开式

$$1+xy+x^2y^2+\cdots=\frac{1}{1-xy}$$

或者反过来

$$\frac{1}{1-xy}=\sum_{n=0}^{\infty}x^ny^n$$

因而

$$\int_0^1\int_0^1\frac{\mathrm{d}x\mathrm{d}y}{1-xy}=\int_0^1\int_0^1\sum_{n=0}^{\infty}x^ny^n\mathrm{d}x\mathrm{d}y=\sum_{n=0}^{\infty}\int_0^1x^n\mathrm{d}x\int_0^1y^n\mathrm{d}y=$$

$$\sum_{n=1}^{\infty}\left(\frac{x^{n+1}}{n+1}\right)\Big|_0^1\left(\frac{y^{n+1}}{n+1}\right)\Big|_0^1=\sum_{n=0}^{\infty}\frac{1}{(n+1)^2}=$$

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \zeta(2)$$

引理 12.5.3 $\zeta(2) = \frac{\pi^2}{6}$。

证明 考虑积分 $I = \int_0^1\int_0^1 \frac{\mathrm{d}x\mathrm{d}y}{1 - xy}, J = \int_0^1\int_0^1 \frac{\mathrm{d}x\mathrm{d}y}{1 + xy}$,那么

$$I - J = \int_0^1\int_0^1 \left(\frac{1}{1 - xy} - \frac{1}{1 + xy}\right)\mathrm{d}x\mathrm{d}y = \int_0^1\int_0^1 \frac{2xy}{1 - x^2y^2}\mathrm{d}x\mathrm{d}y$$

在上面的积分中令 $u = x^2, v = y^2$,那么在正方形$[0,1;0,1]$中,$x = \sqrt{u}, y = \sqrt{v}$。变换的雅可比行列式为

$$\frac{D(x,y)}{D(u,v)} = \begin{vmatrix} x_u' & x_v' \\ y_u' & y_v' \end{vmatrix} = \begin{vmatrix} \frac{1}{2\sqrt{u}} & 0 \\ 0 & \frac{1}{2\sqrt{v}} \end{vmatrix} = \frac{1}{4\sqrt{uv}}$$

而
$$I - J = \int_0^1\int_0^1 \frac{2\sqrt{uv}}{1 - uv} \cdot \frac{\mathrm{d}u\mathrm{d}v}{4\sqrt{uv}} = \frac{1}{2}\int_0^1\int_0^1 \frac{\mathrm{d}u\mathrm{d}v}{1 - uv} = \frac{1}{2}I$$

故
$$\frac{1}{2}I - J = 0$$

另一方面

$$I + J = \int_0^1\int_0^1 \left(\frac{1}{1 - xy} + \frac{1}{1 + xy}\right)\mathrm{d}x\mathrm{d}y = 2\int_0^1\int_0^1 \frac{\mathrm{d}x\mathrm{d}y}{1 - x^2y^2}$$

把上面两式相加即得

$$\frac{3}{4}I = \int_0^1\int_0^1 \frac{\mathrm{d}x\mathrm{d}y}{1 - x^2y^2}$$

在上面的积分中再作变换 $T: x = \frac{\sin\theta}{\cos\varphi}, y = \frac{\sin\varphi}{\cos\theta}$,那么

$$xy = \tan\theta\tan\varphi, \sin\theta = x\cos\varphi, \cos\theta = \frac{\sin\varphi}{y}$$

故
$$x^2\cos^2\varphi + \frac{\sin^2\varphi}{y^2} = 1, x^2 + \frac{\tan^2\varphi}{y^2} = \frac{1}{\cos^2\varphi} = 1 + \tan^2\varphi$$

因此
$$\left(\frac{1}{y^2} - 1\right)\tan^2\varphi = 1 - x^2, \tan\varphi = \sqrt{\frac{1 - x^2}{\frac{1}{y^2} - 1}} = y\sqrt{\frac{1 - x^2}{1 - y^2}}$$

$$\tan\theta = x\sqrt{\frac{1 - x^2}{1 - y^2}}$$

沿着线段 $x = 0, 0 \leqslant y \leqslant 1, \tan\varphi = \frac{y}{\sqrt{1 - y^2}}$。因此当 $y \to 0$ 时,$\tan\varphi \to 0$,当 $y \to 1$ 时,$\tan\varphi \to +\infty$。这说明变换 T 把线段$x = 0, 0 \leqslant y \leqslant 1$变为线段$0 \leqslant \varphi \leqslant$

$\frac{\pi}{2},\theta=0$。同理变换 T 把线段 $0\leqslant x\leqslant 1,y=0$ 变为线段 $\varphi=0,0\leqslant\theta\leqslant\frac{\pi}{2}$。

当 $xy=k$ 时，$0<k<1$ 时。$\tan\theta\tan\varphi=k$ 这是 $\varphi-\theta$ 平面上一条联结 $\left(0,\frac{\pi}{2}\right)$ 和 $\left(\frac{\pi}{2},0\right)$ 两点而向下凹的曲线，因此变换 T 把双曲线 $xy=k,0<k<1$ 变为 $\varphi-\theta$ 平面上具有共同顶点 $\left(0,\frac{\pi}{2}\right)$ 和 $\left(\frac{\pi}{2},0\right)$ 的曲线 $\tan\theta\tan\varphi=k,0<k<1$。

当 $xy=1$ 时，$x=1,y=1$。这时 $\sin\theta=\cos\varphi,\sin\varphi=\cos\theta$，因此 $\theta+\varphi=\frac{\pi}{2}$，即变换 T 把点 $(1,1)$ 变为线段 $\theta+\varphi=\frac{\pi}{2},0\leqslant\varphi\leqslant\frac{\pi}{2}$。

以上讨论说明变换 T 把 $x-y$ 平面上以 $(0,0),(0,1),(1,0),(1,1)$ 为顶点的正方形变为 $\varphi-\theta$ 平面上以 $(0,0),\left(0,\frac{\pi}{2}\right),\left(\frac{\pi}{2},0\right)$ 为顶点的等边直角三角形（图 12.5.1）。

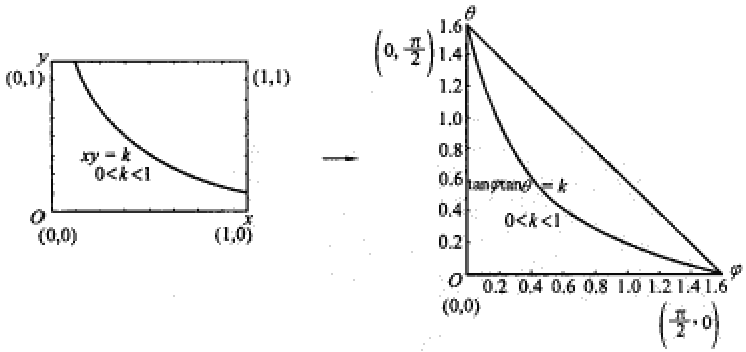


图 12.5.1　变换 T 的作用

又

$$\frac{D(x,y)}{D(\varphi,\theta)}=\begin{vmatrix}x_\varphi' & y_\varphi'\\ x_\theta' & y_\theta'\end{vmatrix}=\begin{vmatrix}\dfrac{\cos\theta}{\cos\varphi} & -\dfrac{\sin\varphi(-\sin\theta)}{\cos^2\varphi}\\ -\dfrac{\sin\theta(-\sin\varphi)}{\cos^2\varphi} & \dfrac{\cos\varphi}{\cos\theta}\end{vmatrix}=1-\tan^2\theta\tan^2\varphi$$

因而

$$\frac{3}{4}I=\int_0^1\int_0^1\frac{\mathrm{d}x\mathrm{d}y}{1-x^2y^2}=\int_0^{\frac{\pi}{2}}\int_0^{\frac{\pi}{2}-\theta}\frac{1}{1-\tan^2\varphi\tan^2\theta}(1-\tan^2\varphi\tan^2\theta)\mathrm{d}\varphi\mathrm{d}\theta=$$

$$\int_0^{\frac{\pi}{2}}\int_0^{\frac{\pi}{2}-\theta}\mathrm{d}\varphi\mathrm{d}\theta=\int_0^{\frac{\pi}{2}}\left(\frac{\pi}{2}-\theta\right)\mathrm{d}\theta=\left(\frac{\pi}{2}\theta-\frac{1}{2}\theta^2\right)\Big|_0^{\frac{\pi}{2}}=$$
$$\frac{\pi^2}{4}-\frac{\pi^2}{8}=\frac{\pi^2}{8}$$

因此由引理 12.5.2 即得

$$\zeta(2)=I=\frac{4}{3}\cdot\frac{\pi^2}{8}=\frac{\pi^2}{6}$$

引理 12.5.4 $\int_0^1 u^k\ln u\mathrm{d}u=-\frac{1}{(k+1)^2}, k>0$。

证明 由分部积分得出

$$\int_0^1 uk\ln u\mathrm{d}u=\frac{u^{k+1}}{k+1}\ln u\Big|_0^1-\frac{1}{k+1}\int_0^1 u^{k+1}\frac{\mathrm{d}u}{u}=-\frac{1}{k+1}\cdot\frac{u^{k+1}}{k+1}\Big|_0^1=$$
$$-\frac{1}{(k+1)^2}$$

引理 12.5.5 $\int_0^1\int_0^1 x^py^q\mathrm{d}x\mathrm{d}y=\frac{1}{(p+1)(q+1)}, 1\leqslant p\leqslant n-1, 1\leqslant q\leqslant n-1$。

证明
$$\int_0^1\int_0^1 x^py^q\mathrm{d}x\mathrm{d}y=\int_0^1 x^p\mathrm{d}x\int_0^1 y^q\mathrm{d}y=\frac{x^{p+1}}{p+1}\Big|_0^1\frac{y^{q+1}}{q+1}\Big|_0^1=$$
$$\frac{1}{(p+1)(q+1)}$$

引理 12.5.6 $\int_0^1\int_0^1\frac{x^p}{1-xy}\mathrm{d}x\mathrm{d}y=\sum_{k=1}^{k=p}(-1)^{k-1}C_{p-1}^{k-1}\frac{1}{k^2}, p\geqslant 1$。

证明
$$\int_0^1\int_0^1\frac{x^p}{1-xy}\mathrm{d}x\mathrm{d}y=\int_0^1 x^p\mathrm{d}x\int_0^1\frac{\mathrm{d}y}{1-xy}=\int_0^1 x^p\left(\frac{\ln(1-xy)}{-x}\Big|_{y=0}^{y=1}\right)\mathrm{d}x=$$
$$-\int_0^1 x^{p-1}\ln(1-x)\mathrm{d}x\text{（在此积分中令 }1-x=u\text{，那么 }\mathrm{d}x=-\mathrm{d}u\text{）}=$$
$$-\int_1^0(1-u)^p\ln u(-\mathrm{d}u)=-\int_0^1(1-u)^p\ln u\mathrm{d}u=$$
$$-\int_0^1\sum_{k=0}^{k=p-1}(-1)^kC_{p-1}^ku^k\ln u\mathrm{d}u=$$
$$-\sum_{k=0}^{k=p-1}(-1)^kC_{p-1}^k\int_0^1u^k\ln u\mathrm{d}u\text{（由引理 12.5.4）}=$$
$$-\sum_{k=0}^{k=p-1}(-1)^kC_{p-1}^k\left(-\frac{1}{(k+1)^2}\right)\text{（在此和式中令 }i+1=k\text{）}=$$
$$\sum_{k=1}^{k=p}(-1)^{k-1}C_{p-1}^{k-1}\frac{1}{k^2}$$

引理 12.5.7 $\int_0^1\int_0^1\frac{y^q}{1-xy}\mathrm{d}x\mathrm{d}y=\sum_{k=1}^{k=q}(-1)^{k-1}C_{q-1}^{k-1}\frac{1}{k^2}, q\geqslant 1$。

证明　与引理 12.5.6 类似。

引理 12.5.8

$$\int_0^1\int_0^1 \frac{x^r y^s}{1-xy}\mathrm{d}x\mathrm{d}y = \begin{cases} \sum\limits_{\substack{1\leqslant p\leqslant r-1\\1\leqslant q\leqslant s-1}} \dfrac{a_{pq}}{(p+1)(q+1)} + \sum\limits_{k=1}^{r}\dfrac{b_k}{k^2} + \sum\limits_{k=1}^{s}\dfrac{c_k}{k^2} + c\zeta(2), & r \neq s \\ \zeta(2) - \sum\limits_{k=1}^{r}\dfrac{1}{k^2}, & r = s \end{cases}$$

其中 a_{pq}, b_k, c_k, c 都是整数。

证明　(1) 当 $r \neq s$ 时，上述积分可以通过 $x^r y^s$ 除以 $xy-1$ 的除法而重新组合成以下四种类型的积分的和：

类型 Ⅰ：$\int_0^1\int_0^1 x^p y^q \mathrm{d}x\mathrm{d}y, 1 \leqslant p \leqslant r-1, 1 \leqslant q \leqslant s-1$；

类型 Ⅱ：$\int_0^1\int_0^1 \frac{x^p}{1-xy}\mathrm{d}x\mathrm{d}y, 1 \leqslant p \leqslant r$；

类型 Ⅲ：$\int_0^1\int_0^1 \frac{y^q}{1-xy}\mathrm{d}x\mathrm{d}y, 1 \leqslant q \leqslant s$；

类型 Ⅳ：$\int_0^1\int_0^1 \frac{\mathrm{d}x\mathrm{d}y}{1-xy}$。

由引理 12.5.2、引理 12.5.5、引理 12.5.6 和引理 12.5.7 可知，引理中的积分是形如$\frac{1}{(p+1)(q+1)}, 1 \leqslant p \leqslant r-1, 1 \leqslant q \leqslant s-1, \frac{1}{k^2}(k = 1,2,\cdots,r)$，$\frac{1}{k^2}(k = 1,2,\cdots,s)$ 和 $\zeta(2)$ 的整数线性组合，这就证明了引理的第一部分。

(2) 当 $r = s$ 时

$$\int_0^1\int_0^1 \frac{x^r y^r}{1-xy}\mathrm{d}x\mathrm{d}y = \int_0^1\int_0^1 x^r y^r \sum_{k=0}^{\infty} x^k y^k \mathrm{d}x\mathrm{d}y = \sum_{k=r}^{\infty}\int_0^1 x^k \mathrm{d}x \int_0^1 y^k \mathrm{d}y =$$

$$\sum_{k=r}^{\infty}\left(\frac{x^{k+1}}{k+1}\bigg|_0^1\right)\left(\frac{y^{k+1}}{k+1}\bigg|_0^1\right) = \sum_{k=r}^{\infty}\frac{1}{(k+1)^2} =$$

$$\sum_{k=1}^{\infty}\frac{1}{k^2} - \sum_{k=1}^{r}\frac{1}{k^2} = \zeta(2) - \sum_{k=1}^{r}\frac{1}{k^2}$$

引理 12.5.9

$$\int_0^1 x^m \int_0^1 \frac{(1-y)^n}{1-xy}\mathrm{d}x\mathrm{d}y = \sum_{\substack{0\leqslant p\leqslant m-1\\0\leqslant q\leqslant n-1}} \frac{a_{pq}}{(p+1)(q+1)} + \sum_{k=1}^{m}\frac{b_k}{k^2} + \sum_{k=1}^{n}\frac{c_k}{k^2} + c\zeta(2)$$

$$0 \leqslant m \leqslant n$$

证明　把 $(1-y)^n$ 做二项式展开，所说的积分即化为形如

$$\int_0^1\int_0^1 \frac{x^m y^s}{1-xy}\mathrm{d}x\mathrm{d}y, 0 \leqslant s \leqslant n$$

的积分的整系数线性组合，再由引理 12.5.8 即知引理成立。

引理 12.5.10 设 $P_n(x)$ 是区间[0,1]上的勒让德多项式

$$f(x)=\int_0^1\frac{(1-y)^n}{1-xy}\mathrm{d}y$$

那么

$$\int_0^1 P_n(x)f(x)\mathrm{d}x=\frac{A_n+B_n\zeta(2)}{d_n^2}$$

其中 A_n 和B_n 都是依赖于n 的整数。$d_n=[1,2,\cdots,n]$是前 n 个自然数 $1,2,\cdots,n$ 的最小公倍数。

证明 由引理12.1.4知 $P_n(x)$ 是 $1,x,x^2,\cdots,x^n$ 的整系数线性组合，因此由引理 12.5.9 即得

$$\int_0^1 P_n(x)f(x)\mathrm{d}x=\sum_{\substack{1\leqslant p\leqslant n\\ 1\leqslant q\leqslant n}}\frac{a_{pq}}{pq}+\sum_{k=1}^{n}\frac{b_k}{k^2}+c_n\zeta(2)$$

上式中各分数的最小公倍数显然是 d_n^2，由此就得出引理。

引理 12.5.11 设 $f(x)=\int_0^1\frac{(1-y)^n}{1-xy}\mathrm{d}y$，那么

$$\frac{\mathrm{d}^n}{\mathrm{d}x^n}f(x)=(-1)^n n!\int_0^1\frac{y^n(1-y)^n}{(1-xy)^{n+1}}\mathrm{d}y$$

证明 $\frac{\mathrm{d}^n}{\mathrm{d}x^n}f(x)=\frac{\mathrm{d}^n}{\mathrm{d}x^n}\int_0^1\frac{(1-y)^n}{1-xy}\mathrm{d}y=\frac{\mathrm{d}^n}{\mathrm{d}x^n}\int_0^1(1-y)^n(1-xy)^{-1}\mathrm{d}y=$

$$\int_0^1(1-y)^n(-y)(-2y)\cdots(-ny)(1-xy)^{-n-1}\mathrm{d}y=$$

$$(-1)^n n!\int_0^1\frac{y^n(1-y)^n}{(1-xy)^{n+1}}\mathrm{d}y$$

引理 12.5.12 设 $q=\frac{\sqrt{5}-1}{2}$，那么在正方形 $\Omega=[0,1;0,1]$上

$$0\leqslant f(x,y)=\frac{xy(1-x)(1-y)}{1-xy}\leqslant q^5$$

证明 由于在 Ω 的边界 $\partial\Omega$ 上，$f(x,y)=0$，因此 $f(x,y)$ 的最大值只可能在 Ω 的内部达到，也就是说 $f(x,y)$ 在 Ω 上的最大值只可能是 Ω 内的某个极大值。

$$\frac{\partial f}{\partial x}=y(1-y)\frac{\partial}{\partial x}\frac{x(1-x)}{1-xy}=\frac{y(1-y)(1-2x+x^2y)}{(1-xy)^2}$$

$$\frac{\partial f}{\partial y}=x(1-x)\frac{\partial}{\partial y}\frac{y(1-y)}{1-xy}=\frac{x(1-x)(1-2x+x^2y)}{(1-xy)^2}$$

方程组$\frac{\partial f}{\partial x}=0,\frac{\partial f}{\partial y}=0$ 的位于 Ω 内部的解由方程组

$$\begin{cases}1-2x+x^2y=0\\ 1-2y+x^2y=0\end{cases}$$

给出。将上面的两个方程相减得$(x-y)(2-xy)=0$。由于在 Ω 内 $xy-2\neq 0$，故由此得 $y=x$，把 $y=x$ 代入 $1-2x+x^2y$ 得

$$x^3-2x+1=(x-1)(x^2+x-1)=0$$

由于在 Ω 内 $x\neq 1$，由此得 $x=\frac{-1\pm\sqrt{5}}{2}$。舍去位于 Ω 之外的根$\frac{-1-\sqrt{5}}{2}$就得到方程组$\frac{\partial f}{\partial x}=0,\frac{\partial f}{\partial y}=0$在 Ω 内的唯一解是 $x=y=q$，由于 $f(q,q)>f(0,0)=0$，因此 $f(q,q)$ 是 $f(x,y)$ 在 Ω 内的唯一极大值，也就是 $f(x,y)$ 在 Ω 上的最大值。

q 满足方程 $q^2+q-1=0$ 或 $1-q=q^2$ 及 $1-q^2=q$。而

$$f(q,q)=\frac{q\cdot q\cdot(1-q)\cdot(1-q)}{1-q^2}=\frac{q^2\cdot q^2\cdot q^2}{1-q^2}=\frac{q^6}{q}=q^5$$

故在 Ω 上

$$0\leqslant f(x,y)\leqslant q^5$$

定理 12.5.1 $\zeta(2)$ 是无理数。

证明 设 $\zeta(2)$ 不是无理数，那么 $\zeta(2)=\frac{a}{b}$，其中 a,b 是互素的正整数。由引理 12.5.10 知 bd_n^2I 是一个整数，其中 $I=\int_0^1 P_n(x)f(x)\mathrm{d}x$。但是

$$|bd_n^2I|=\left|bd_n^2\int_0^1\left(\frac{\mathrm{d}^n}{\mathrm{d}x^n}\frac{1}{n!}x^n(1-x)^n\int_0^1\frac{(1-y)^n}{1-xy}\mathrm{d}y\right)\mathrm{d}x\right|=$$

$$\left|bd_n^2\int_0^1\left(\frac{1}{n!}x^n(1-x)^n\frac{\mathrm{d}^n}{\mathrm{d}x^n}\int_0^1\frac{(1-y)^n}{1-xy}\mathrm{d}y\right)\mathrm{d}x\right|=$$

$$\left|bd_n^2\int_0^1\frac{1}{n!}x^n(1-x)^n\int_0^1\frac{y^n(1-y)^n}{(1-xy)^{n+1}}(-1)^n n!\,\mathrm{d}x\mathrm{d}y\right|=$$

(引理 12.5.11)

$$\left|bd_n^2\int_0^1\int_0^1\left(\frac{x(1-x)y(1-y)}{1-xy}\right)^n\frac{1}{1-xy}\mathrm{d}x\mathrm{d}y\right|$$

显然，上述积分是正的，且由引理 12.5.12 知

$$\frac{x(1-x)y(1-y)}{1-xy}$$

在 $\Omega=[0,1;0,1]$ 上于 $x=y=q$ 处达到最大值q^5，因此由引理 12.5.2 和定理 3.8.14 就得出当 $n\to\infty$ 时

$$0<|bd_n^2I|<bd_n^2\int_0^1\int_0^1\left(\frac{\sqrt{5}-1}{2}\right)^{5n}\frac{1}{1-xy}\mathrm{d}x\mathrm{d}y<b3^n\left(\frac{\sqrt{5}-1}{2}\right)^{5n}\int_0^1\int_0^1\frac{\mathrm{d}x\mathrm{d}y}{1-xy}\leqslant$$

$$b\zeta(2)3^n\left(\frac{\sqrt{5}-1}{2}\right)^{5n}\leqslant b\,\frac{a}{b}3^n\left(\frac{\sqrt{5}-1}{2}\right)^{5n}\leqslant a3^n\left(\frac{\sqrt{5}-1}{2}\right)^{5n}\to 0$$

这就与 bd_n^2I 是一个正整数的性质相矛盾，所得的矛盾就说明 $\zeta(2)$ 必是一个无理数。

12.6 最新的记录：$\zeta(3)$ 的无理性

在这一节中，我们要证明 $\zeta(3)$ 的无理性，虽然在方法上与前几节有类似之处，但是这一结果的难度和性质、意义却和前几节完全不同。原因在于从定理3.8.8(3) 我们已经知道

$$B_{2n} = (-1)^{n-1}\frac{2(2n)!}{(2\pi)^{2n}}\zeta(2n)$$

其中 $\zeta(2n) = \sum_{k=1}^{\infty}\frac{1}{k^{2n}}$。而 B_{2n} 是所谓贝努利数，是一个有理数。因此 $\zeta(2n)$ 和 π^{2n} 只差一个有理系数。以后我们还要证明 π 的超越性。这些结果是欧拉、贝努利以及林德曼等人早在十七八世纪中就已获得和解决的问题。由 π 的超越性我们立刻可以推出 π^{2n} 不可能是一个有理数，否则 π 将是一个代数数。而由此及关系式 $\zeta(2n) = \sum_{k=1}^{\infty}\frac{1}{k^{2n}}$ 即可得出 $\zeta(2),\zeta(4),\cdots,\zeta(2n),\cdots$ 都是无理数。因此关于 $\zeta(2)$ 的无理性是一个早已解决的问题，而且是批量性质解决的。我们在上一节中介绍的方法其性质相当于有些问题用高等数学方法早已解决，但是如果有人能不用高等数学方法而用更初等的知识将其解决，也是很有趣味和意义的。因为我们从思维的直觉上有一种自然而然的感觉，要用尽可能简单和初等的知识和方法去解决问题。因此如果有人有一天发现在高等数学或很高深领域中的一个问题其实本来可以用较简单和初等的知识和方法来解决，大家都会觉得这是很优美和令人舒服的结果。当然这些并不能改变这一问题可能是早已解决的事实和本质。

和 $\zeta(2n)$ 不同，对于 $\zeta(2n+1) = 1 + \frac{1}{2^{2n+1}} + \frac{2}{2^{2n+1}} + \cdots$ 这些式子，除了可以用近似计算的方法得知它们的近似值外，我们并无类似 $B_{2n} = (-1)^{n-1}\cdot\frac{2(2n)!}{(2\pi)^{2n}}\zeta(2n)$ 这样的关系式，对其其他性质也所知甚少。乃至到1978年之前，即使确定一下它们的无理性和有理性也非常困难。直到1978年，在芬兰赫尔辛基举行的世界数学家大会上，法国数学家阿皮瑞(Apery)宣布他证明了 $\zeta(3)$ 的无理性。这大大出乎数学大师们的预料，这是一个最新的突破，但这一结果至今还未能获得新的突破。这句话的意思是，虽然我们现在已能证明的无理性，但是至今还不能知道 $\zeta(5),\zeta(7),\cdots$ 等数是无理的还是有理的。

就像在12.5中一样，我们首先要给出一些和 $\zeta(3)$ 有关的关系式。

引理 12.6.1 $\zeta(3) = -\frac{1}{2}\int_0^1\int_0^1\frac{\ln xy}{1-xy}\mathrm{d}x\mathrm{d}y$。

证明 $\int_0^1\int_0^1 \frac{\ln xy}{1-xy}\mathrm{d}x\mathrm{d}y = \int_0^1\int_0^1\sum_{k=0}^{\infty} x^k y^k \ln xy\mathrm{d}x\mathrm{d}y =$

$$\int_0^1\int_0^1\sum_{k=0}^{\infty} x^k y^k(\ln x+\ln y)\mathrm{d}x\mathrm{d}y =$$

$$\int_0^1\int_0^1\sum_{k=0}^{\infty} x^k y^k \ln x\mathrm{d}x\mathrm{d}y + \int_0^1\int_0^1\sum_{k=0}^{\infty} x^k y^k \ln y\mathrm{d}x\mathrm{d}y =$$

$$\sum_{k=0}^{\infty}\int_0^1\int_0^1 x^k y^k \ln x\mathrm{d}x\mathrm{d}y + \sum_{k=0}^{\infty}\int_0^1\int_0^1 x^k y^k \ln y\mathrm{d}x\mathrm{d}y =$$

$$2\sum_{k=0}^{\infty}\int_0^1\int_0^1 x^k y^k \ln x\mathrm{d}x\mathrm{d}y = 2\sum_{k=0}^{\infty}\int_0^1 x^k\ln x\mathrm{d}x\int_0^1 y^k\mathrm{d}y =$$

$$2\sum_{k=0}^{\infty}\left(\frac{x^{k+1}}{k+1}\ln x\Big|_0^1 - \frac{1}{k+1}\int_0^1 x^{k+1}\frac{\mathrm{d}x}{x}\right)\left(\frac{y^{k+1}}{k+1}\right)\Big|_0^1 =$$

$$-2\sum_{k=0}^{\infty}\frac{1}{(k+1)^2}\int_0^1 x^k\mathrm{d}x = -2\sum_{k=0}^{\infty}\frac{1}{(k+1)^3} =$$

$$-2\sum_{k=1}^{\infty}\frac{1}{k^3} = -2\zeta(3)$$

由此即可得出引理。

引理 12.6.2 $\int_0^1\int_0^1\int_0^1 \frac{\mathrm{d}x\mathrm{d}y\mathrm{d}z}{1-(1-xy)z} = 2\zeta(3)$。

证明 $\int_0^1\int_0^1\int_0^1 \frac{\mathrm{d}x\mathrm{d}y\mathrm{d}z}{1-(1-xy)z} = \int_0^1\int_0^1\left(\int_0^1\frac{\mathrm{d}z}{1-(1-xy)z}\right)\mathrm{d}x\mathrm{d}y =$

$$\int_0^1\int_0^1\left(-\frac{\ln(1-(1-xy)z)}{1-xy}\Big|_0^1\right)\mathrm{d}x\mathrm{d}y =$$

$$-\int_0^1\int_0^1\frac{\ln xy}{1-xy}\mathrm{d}x\mathrm{d}y = 2\zeta(3)$$

引理 12.6.3 $\frac{x^r y^s}{1-xy}\ln xy = \left(\frac{\mathrm{d}}{\mathrm{d}t}\frac{x^{r+t}y^{s+t}}{1-xy}\right)\Big|_{t=0}$。

证明 $\frac{\mathrm{d}}{\mathrm{d}t}\frac{x^{r+t}y^{s+t}}{1-xy} = \frac{(\ln x)x^{r+t}y^{s+t}+(\ln y)x^{r+t}y^{s+t}}{1-xy} =$

$$\frac{x^{r+t}y^{s+t}(\ln x+\ln y)}{1-xy} = \frac{x^{r+t}y^{s+t}\ln xy}{1-xy}$$

故
$$\left(\frac{\mathrm{d}}{\mathrm{d}t}\frac{x^{r+t}y^{s+t}}{1-xy}\right)\Big|_{t=0} = \frac{x^r y^s\ln xy}{1-xy}$$

引理 12.6.4 (1) 当 $r\neq s$ 时

$$\int_0^1\int_0^1\frac{x^r y^s\ln xy}{1-xy}\mathrm{d}x\mathrm{d}y = -\sum_{\substack{1\leqslant p\leqslant r-1\\ 1\leqslant q\leqslant s-1}}\left(\frac{a_{pq}}{(p+1)^2(q+1)}+\frac{a_{pq}}{(p+1)(q+1)^2}\right) - 2\sum_{k=1}^{r}\frac{b_k}{k^3} - 2\sum_{k=1}^{s}\frac{c_k}{k^3} + c\zeta(3)$$

(2) 当 $r = s$ 时

$$\int_0^1\int_0^1 \frac{x^r y^s \ln xy}{1-xy}\mathrm{d}x\mathrm{d}y = -2\sum_{k=1}^{r}\frac{1}{k^3} - 2\zeta(3)$$

证明 (1) 当 $r \neq s$ 时,所说的积分可通过引理 12.6.3 及积分号与微分号的交换化为积分 $\frac{\mathrm{d}}{\mathrm{d}t}\int_0^1\int_0^1 \frac{x^{r+t}y^{s+t}}{1-xy}\mathrm{d}x\mathrm{d}y\Big|_{t=0}$ 与积分 $\int_0^1\int_0^1 \frac{\ln xy}{1-xy}\mathrm{d}x\mathrm{d}y$ 的组合。再由引理 12.5.8 和引理 12.6.1 以及关系式

$$\frac{\mathrm{d}}{\mathrm{d}t}\frac{1}{(p+t+1)(q+t+1)} = -\left(\frac{1}{(p+t+1)^2(q+t+1)} + \frac{1}{(p+t+1)(q+t+1)^2}\right)$$

和
$$\frac{\mathrm{d}}{\mathrm{d}t}\frac{1}{(k+t)^2} = -\frac{2}{(k+t)^3}$$

即可得出引理的部分(1)。

(2) 当 $r = s$ 时,由引理 12.6.3 和引理 12.5.8 的证明得

$$\int_0^1\int_0^1 \frac{x^r y^s \ln xy}{1-xy}\mathrm{d}x\mathrm{d}y = \int_0^1\int_0^1 \frac{\mathrm{d}}{\mathrm{d}t}\frac{x^{r+t}y^{s+t}}{1-xy}\Big|_{t=0}\mathrm{d}x\mathrm{d}y = \sum_{k=r+t}\frac{\mathrm{d}}{\mathrm{d}t}\frac{1}{k^2}\Big|_{t=0} = \sum_{k=r+t} - \frac{2}{k^3} = 2\left(\sum_{k=1}^{r}\frac{1}{k^3} - \sum_{k=1}^{\infty}\frac{1}{k^3}\right) = 2\sum_{k=1}^{r}\frac{1}{k^3} - 2\zeta(3)$$

引理 12.6.5 设 $P_n(x)$ 表示区间[0,1]上的勒让德多项式,那么

$$\int_0^1 x^m\int_0^1 \frac{P_n(y)\ln xy}{1-xy}\mathrm{d}x\mathrm{d}y = \sum_{\substack{1\leqslant p\leqslant n-1\\ 1\leqslant q\leqslant n-1}}\left(\frac{a_{pq}}{(p+1)^2(q+1)} + \frac{a_{pq}}{(p+1)(q+1)^2}\right) + \sum_{k=1}^{m}\frac{b_k}{k^3} + \sum_{k=1}^{n}\frac{c_k}{k^3} + c\zeta(3)$$

证明 把 $P_n(y)$ 展开,所说的积分即成为形如

$$\int_0^1\int_0^1 \frac{x^m y^s \ln xy}{1-xy}\mathrm{d}x\mathrm{d}y$$

的积分的整系数的线性组合,再由引理 12.6.5 即知引理成立。

引理 12.6.6 设 $f(x) = \int_0^1 \frac{P_n(y)}{1-xy}\ln xy\mathrm{d}x\mathrm{d}y$,那么

$$\int_0^1 f(x)P_n(x)\mathrm{d}x = \frac{A_n + B_n\zeta(3)}{d_n^3}$$

其中 $P_n(x)$,$P_n(y)$ 是区间[0,1]上的勒让德多项式,A_n 和 B_n 都是依赖于 n 的整数。$d_n = [1,2,\cdots,n]$ 是前 n 个自然数 $1,2,\cdots,n$ 的最小公倍数。

证明 由引理 12.1.4 知 $P_n(x)$ 是 $1,x,x^2,\cdots,x^n$ 的整系数线性组合,$P_n(y)$ 是 $1,y,y^2,\cdots,y^n$ 的整系数线性组合,因此由引理 12.6.5 即得

$$\int_0^1 P_n(x)f(x)\mathrm{d}x = \sum_{\substack{1\leqslant p\leqslant n\\1\leqslant q\leqslant n}}\left(\frac{a_{pq}}{p^2q}+\frac{a_{pq}}{pq^2}\right)+\sum_{k=1}^{m}\frac{b_k}{k^3}+c_n\zeta(3)$$

上式中各分数的最小公倍数显然是 d_n^3，由此就得出引理。

引理 12.6.7 设 $q=\sqrt{2}-1$，那么在正方体 $\Omega=[0,1]^3$ 上

$$0\leqslant f(x,y,z)=\frac{xyz(1-x)(1-y)(1-z)}{1-(1-xy)z}\leqslant q^4$$

证明 由于在 Ω 的边界 $\partial\Omega$ 上，$f(x,y,z)=0$，因此 $f(x,y,z)$ 的最大值只可能在 Ω 的内部达到，也就是说 $f(x,y,z)$ 在 Ω 上的最大值只可能是 Ω 内的某个极大值。

$$\frac{\partial f}{\partial x}=\frac{yz(1-y)(1-z)((1-2x)(1-z+xyz)-yz(x-x^2))}{(1-z+xyz)^2}=$$

$$\frac{yz(1-y)(1-z)(1-2x-z+2xz-x^2yz)}{(1-z+xyz)^2}$$

$$\frac{\partial f}{\partial y}=\frac{xz(1-x)(1-z)(1-2y-z+2yz-xy^2z)}{(1-z+xyz)^2}$$

$$\frac{\partial f}{\partial z}=\frac{xy(1-x)(1-y)(1-2z+z^2-xyz^2)}{(1-z+xyz)^2}$$

由于在 Ω 内 $x>0,y>0,z>0,1-x>0,1-y>0,1-z>0$，因此方程组 $\frac{\partial f}{\partial x}=\frac{\partial f}{\partial y}=\frac{\partial f}{\partial z}=0$ 在 Ω 内的解可由方程组

$$\begin{cases}1-2x-z+2xz-x^2yz=0\\1-2y-z+2yz-xy^2z=0\\1-2z+z^2-xyz^2=0\end{cases}$$

决定。在上面的方程组中，用第二式减去第一式得

$$(2(1-z)+xyz)(x-y)=0$$

由于在 Ω 内，$2(1-z)+xyz>0$，因此由上式就得出 $y=x$，把 $y=x$ 代入第三式中得

$$(1-z)^2=x^2z^2$$

由于在 Ω 内，$1-z>0,xz>0$，因此由上式就得出 $1-z=xz$，由此解出

$$z=\frac{1}{1+x}$$

把 $y=x$ 和上式代入方程组的第一式得

$$1-2x-\frac{1}{1+x}+\frac{2x}{1+x}-\frac{x^3}{1+x}=0$$

上式两边都乘以在 Ω 内为正的数 $1+x$ 就得出

$$x^3+2x^2-x=0$$

由于在 Ω 内，$x > 0$，因此由上式就得出 $x^2 + 2x - 1 = 0$，此方程在 Ω 内的唯一解是 $x = q = \sqrt{2} - 1$。把 $x = q$ 代入 $y = x$ 和 $z = \frac{1}{1+x}$ 就得出方程组 $\frac{\partial f}{\partial x} = \frac{\partial f}{\partial y} = \frac{\partial f}{\partial z} = 0$ 在 Ω 内的唯一解是 $x = y = q, z = \frac{1}{1+q}$。$q$ 满足方程 $q^2 + 2q - 1 = 0$，因此

$$1 - q = q + q^2 = q(1+q)$$

而 $f(x,y,z)$ 在 Ω 上的最大值在 $x = y = q, z = \frac{1}{1+q}$ 处取得。

$$f_{\max} = \frac{q^2(1-q)^2 \frac{1}{1+q}\left(1 - \frac{1}{1+q}\right)}{1 - \frac{1}{1+q} + \frac{q^2}{1+q}} = \frac{q^2(q(1+q))^2 q}{(1+q)(1+q-1+q^2)} =$$

$$\frac{q^5(1+q)^2}{q(1+q^2)} = q^4$$

故在 Ω 上 $0 \leqslant f(x,y,z) \leqslant q^4$。

定理 12.6.1 $\zeta(3)$ 是无理数。

证明 假设 $\zeta(3)$ 不是无理数，那么可设 $\zeta(3) = \frac{a}{b}$，其中 a, b 都是正整数。由引理 12.6.6 知 $bd_n^3 I$ 是一个整数，其中 $I = \int_0^1 P_n(x) f(x) \mathrm{d}x$。但是

$$|bd_n^3 I| = \left| bd_n^3 \int_0^1 P_n(x) f(x) \mathrm{d}x \right| = \left| bd_n^3 \int_0^1 P_n(x) \left(\int_0^1 \frac{P_n(y)}{1-xy} \ln xy \mathrm{d}y \right) \mathrm{d}x \right| =$$

$$\left| bd_n^3 \int_0^1 \int_0^1 P_n(x) P_n(y) \left(\int_0^1 \frac{\mathrm{d}z}{1-(1-xy)z} \right) \mathrm{d}x \mathrm{d}y \right| =$$

$$\left| bd_n^3 \int_0^1 \int_0^1 \int_0^1 \frac{P_n(x) P_n(y)}{1-(1-xy)z} \mathrm{d}x \mathrm{d}y \mathrm{d}z \right| =$$

$$\left| bd_n^3 \int_0^1 P_n(y) \int_0^1 P_n(x) \int_0^1 \frac{\mathrm{d}x \mathrm{d}y \mathrm{d}z}{1-(1-xy)z} \right| =$$

$$\left| bd_n^3 \int_0^1 P_n(y) \int_0^1 \frac{x^n(1-x)^n}{n!} \int_0^1 \frac{(-yz)(-2yz)\cdots(-nyz)}{(1-(1-xy)z)^{n+1}} \mathrm{d}x \mathrm{d}y \mathrm{d}z \right| =$$

$$\left| bd_n^3 \int_0^1 \int_0^1 P_n(y) \int_0^1 \frac{x^n(1-x)^n y^n z^n}{(1-(1-xy)z)^{n+1}} \mathrm{d}z \mathrm{d}y \mathrm{d}x \right|$$

在上面的积分中令 $w = \frac{1-z}{1-(1-xy)z}$，那么 $z = \frac{1-w}{1-(1-xy)w}$，$\mathrm{d}z = -\frac{xy}{(1-(1-xy)w)^2}\mathrm{d}w$，因此

$$|bd_n^3 I| = \left| bd_n^3 \int_0^1 \int_0^1 \int_0^1 \frac{(1-x)^n P_n(y)(1-w)^n}{1-(1-xy)w} \mathrm{d}x \mathrm{d}y \mathrm{d}w \right| =$$

$$\left|bd_n^3\int_0^1(1-x)^n\int_0^1 P_n(y)\int_0^1\frac{(1-w)^n}{1-(1-xy)w}\mathrm{d}w\mathrm{d}y\mathrm{d}x\right| =$$

$$\left|bd_n^3\int_0^1(1-x)^n\int_0^1\frac{y^n(1-y)^n}{n!}\cdot\right.$$

$$\left.\int_0^1\frac{(1-w)^n(-xw)(-2xw)\cdots(-nxw)}{(1-(1-xy)w)^{n+1}}\mathrm{d}w\mathrm{d}y\mathrm{d}x\right| =$$

$$\left|bd_n^3\int_0^1\int_0^1\int_0^1\left(\frac{xyw(1-x)(1-y)(1-w)}{1-(1-xy)w}\right)^n\frac{\mathrm{d}x\mathrm{d}y\mathrm{d}w}{1-(1-xy)w}\right| =$$

$$\left|bd_n^3q^{4n}\int_0^1\int_0^1\int_0^1\frac{\mathrm{d}x\mathrm{d}y\mathrm{d}w}{1-(1-xy)w}\right| \leqslant |\,b3^{3n}q^{4n}\zeta(3)\,| \leqslant 2a(3q^4)^n$$

(定理3.8.14)，由上面的不等式就得出当 $n\to\infty$ 时，$bd_n^3I\to 0$。由上面最后一个积分式又可以看出 $|bd_n^3I|>0$，这就与 bd_n^3I 是一个整数相矛盾，所得的矛盾就说明 $\zeta(3)$ 不可能是有理数，因而必是一个无理数。

12.7 e的超越性

埃尔米特(Hermite，charles，1822—1901)，法国数学家．生于洛林地区的迪约兹，卒于巴黎．

引理 12.7.1(埃尔米特恒等式) 设 $f(x)$ 为 m 次的实系数多项式

$$I(z)=\int_0^z e^{z-u}f(u)\mathrm{d}u$$

其中，z 是任意复数，积分沿着0到 z 的直线段，则有

$$I(z)=e^z\sum_{j=0}^m f^{(j)}(0)-\sum_{j=0}^m f^{(j)}(z)$$

证明 由积分学知道

$$\int e^{z-u}\mathrm{d}u=-e^{z-u}$$

由此及分部积分得到

$$I(z)=-e^{z-u}f(u)|_0^z+\int_0^z e^{z-u}f'(u)\mathrm{d}u=-e^0f(z)+e^zf(0)+\int_0^z e^{z-u}f'(u)\mathrm{d}u=$$

$$e^zf(0)-f(z)+\int_0^z e^{z-u}f'(u)\mathrm{d}u=$$

$$e^zf(0)-f(z)+e^zf'(0)-f'(z)+\int_0^z e^{z-u}f''(u)\mathrm{d}u=$$

$$e^zf(0)-f(z)+e^zf'(0)-f'(z)+\cdots+e^zf^{(m)}(0)-f^{(m)}(z)+$$

$\int_0^z e^{z-u}f^{(m+1)}(u)\mathrm{d}u$(由于 $f(x)$ 是 m 次多项式，所以 $f^{(m+1)}(u)\equiv 0$) =

$$e^z(f(0)+f'(0)+\cdots f^{(m)}(0))-(f(z)+f'(z)+\cdots+f^{(m)}(z))=$$

$$e^z\sum_{j=0}^{m}f^{(j)}(0)-\sum_{j=0}^{m}f^{(j)}(z)$$

引理 12.7.2 设 $f^*(x)$ 表示把 $f(x)$ 的系数换成其绝对值所得的多项式，则

$$|I(z)|\leqslant|z|e^{|z|}f^*(|z|)$$

证明
$$|I(z)|=\left|\int_0^z e^{z-u}f(u)\mathrm{d}u\right|\leqslant ML$$

其中 L 是路径：从 0 到 z 的直线段的长度，故 $L=|z|$。$M=\max\limits_{z\in\Gamma}|e^{z-u}f(u)|=|e^{z-\xi}f(\xi)|$，其中 ξ 是路径中某一点。显然

$$|\xi|\leqslant|z|,\ |z-\xi|\leqslant|z|$$

因此

$$\begin{aligned}M=|e^{z-\xi}f(\xi)|\leqslant e^{|z-\xi|}|f(\xi)|\leqslant e^{|z|}|a_0\xi^n+a_1\xi^{n-1}+\cdots+a_n|\leqslant\\ e^{|z|}(|a_0||\xi|^n+|a_1||\xi|^{n-1}+\cdots+|a_n|)\leqslant\\ e^{|z|}(|a_0||z|^n+|a_1||z|^{n-1}+\cdots+|a_n|)\leqslant e^{|z|}f^*(|z|)\end{aligned}$$

故
$$|I(z)|\leqslant|z|e^{|z|}f^*(|z|)$$

引理 12.7.3 设 $f(x)=\dfrac{x^{p-1}(x-1)^p(x-2)^p\cdots(x-n)^p}{(p-1)!}$，其中 $p>n$ 是一个素数，那么

(1) 当 $j<p-1$ 时，$f^{(j)}(0)=f^{(j)}(i)=0,i=1,2,\cdots,n$；

(2) 当 $j=p-1$ 时，$f^{(j)}(0)=(-1)^n(n!)^p$；

(3) 当 $j>p-1$ 时，$f^{(j)}(0)$ 和 $f^{(j)}(i),i=1,2,\cdots,n$ 都是 p 的倍数。

证明 (1)
$$\begin{aligned}f(x)=\frac{x^{p-1}(x-1)^p(x-2)^p\cdots(x-n)^p}{(p-1)!}=\\ x^{p-1}(c_{0,0}x^{np}+c_{0,1}x^{np-1}+\cdots+c_{0,np})=\\ c_{0,0}x^{(n+1)p-1}+c_{0,1}x^{(n+1)p-2}+\cdots+c_{0,np}x^{p-1}\end{aligned}$$

其中

$$c_{0,np}=\frac{((-1)^n)^p(n!)^p}{(p-1)!}=\frac{((-1)^p)^n(n!)^p}{(p-1)!}=\frac{(-1)^n(n!)^p}{(p-1)!}$$

$f(x)$ 的最低项的次数为 $p-1$，因此当 $j<p-1$ 时，$f(x)$ 经过 j 次求导后，得到一个最低项次数为 $p-1-j>0$ 的多项式，由此显然就有 $f^{(j)}(0)=0$。

同理，对任一 $i>0$，把 $f(x)$ 写成 $x-i$ 的多项式后可得 $f(x)$ 是 $x-i$ 的最低项次数为 p 的多项式。因此经过 j 次求导后，得到一个 $x-i$ 的最低项次数为 $p-j>0$ 的多项式，故对任意 $i>0$，有 $f^{(j)}(i)=0$。

(2) 由(1) 中所得的 $f(x)$ 表为 x 的多项式的形式可知，$f(x)$ 经 $p-1$ 次求导后，$f^{(p-1)}(x)$ 是一个常数项为 $(p-1)!c_{0,np}$ 的多项式，因此

$$f^{(p-1)}(0)=(p-1)!c_{0,np}=(-1)^n(n!)^p$$

(3) 设 $m=(n+1)p-1$，由(1)中所得的 $f(x)$ 的形式可写

$$f(x)=\frac{x^m+b_{0,1}x^{m-1}+\cdots+b_{0,m}}{(p-1)!}$$

其中 $b_{0,k}$ 都是整数。当 $j>p-1$ 或 $j\geqslant p$ 时，$f(x)$ 经过 j 次求导后所得的多项式为

$$f^{(j)}(x)=\frac{1}{(p-1)!}\sum_{k=0}^{m-j}b_{0k}A_{m-k}^{j}x^{m-k-j},\ b_{0,0}=1$$

其中 A_{m-k}^{j} 是连续 j 个整数的乘积，因此是 $j!$ 的倍数，因为 $j\geqslant p$，所以也是 $p!$ 的倍数。故 $f^{(j)}(0)$ 和 $f^{(j)}(i)$，$i=1,2,\cdots,n$ 都是 p 的倍数。

引理 12.7.4 如果 $a_ne^n+a_{n-1}e^{n-1}+\cdots+a_0=0$，其中 $a_0,a_1,\cdots,a_n$ 都是整数

$$f(x)=\frac{x^{p-1}(x-1)^p(x-2)^p\cdots(x-n)^p}{(p-1)!}$$

其中 $p>n$ 是一个素数

$$J=a_0I(0)+a_1I(1)+\cdots+a_nI(n)$$

那么

(1) $J=-\sum_{i=0}^{n}\sum_{j=0}^{m}a_if^{(j)}(i)$，其中 $m=(n+1)p-1$ 是 $f(x)$ 的次数；

(2) J 是一个整数，$p\nmid J$。

证明 (1) 由引理 12.7.1 知

$$\begin{aligned}J=a_0I(0)+a_1I(0)+\cdots+a_nI(n)=a_0\Big(\sum_{j=0}^{m}f^{(j)}(0)-\sum_{j=0}^{m}f^{(j)}(0)\Big)+\\ a_1\Big(e\sum_{j=0}^{m}f^{(j)}(0)-\sum_{j=0}^{m}f^{(j)}(1)\Big)+\cdots+\\ a_0\Big(e^n\sum_{j=0}^{m}f^{(j)}(0)-\sum_{j=0}^{m}f^{(j)}(n)\Big)=\\ -\sum_{j=0}^{n}\sum_{j=0}^{m}f^{(j)}(i)\end{aligned}$$

(2) 由引理 12.7.3 知 J 中的项除了 $f^{(p-1)}(0)$ 之外都是 0 或 p 的倍数，故

$$J=f^{(p-1)}(0)+Mp=(-1)^n(n!)^p+Mp$$

是一个整数，但 $p\nmid J$。

定理 12.7.1 e 是一个超越数。

证明 假设 e 不是超越数，那么 e 必满足一个整系数代数方程，因而可设 $a_ne^n+a_{n-1}e^{n-1}+\cdots+a_0=0$，其中 $a_0,a_1,\cdots,a_n$ 都是整数。又设

$$f(x)=\frac{x^{p-1}(x-1)^p(x-2)^p\cdots(x-n)^p}{(p-1)!}$$

其中 $p > n$ 是一个素数

$$J = a_0 I(0) + a_1 I(1) + \cdots + a_n I(n)$$

而

$$I(x) = \int_0^x e^{x-u} f(u) \mathrm{d}u$$

那么由引理 12.7.4 知 J 是一个整数,但是 $p \nmid J$,因此 $J \neq 0$,这说明 $|J| \geqslant 1$。但是另一方面,由引理 12.7.2 知

$$|J| \leqslant |\sum_{i=1}^{n} I(i)| \leqslant |a_i||I(i)| \leqslant \sum_{i=1}^{n} i|a_i| e^i f^*(i) \leqslant \frac{c^p}{(p-1)!}$$

其中 c 是一个与 p 无关的实数,因此当 p 充分大时(由于有无穷多个素数,这是可以办得到的),$|J| < 1$(由于当 $p \to \infty$ 时,$\frac{c^p}{(p-1)!} \to 0$),这与 $|J| \geqslant 1$ 矛盾,所得的矛盾就说明 e 必是一个超越数。

12.8 π的超越性

引理 12.8.1 设 $f(\alpha_1, \alpha_2, \cdots, \alpha_l)$ 是 $\alpha_1, \alpha_2, \cdots, \alpha_l$ 的对称多项式,则当把 f 看成是 $\alpha_1, \alpha_2, \cdots, \alpha_l, 0, 0, \cdots, 0$(其中有任意个 0,比如可设有 $m - l$ 个 0)的多项式时,f 也是它们的对称多项式。

证明 f 是形如 $\alpha_1^{\delta_1}\alpha_2^{\delta_2}\cdots\alpha_l^{\delta_l}$ 的单项式之和,其中 $\delta_1 + \delta_2 + \cdots + \delta_l = k$, $k = 0, 1, 2, \cdots, n$,即

$$f = \sum_{k=0}^{n} \sum_{\delta_1+\delta_2+\cdots+\delta_l=k} a_{\delta_1\delta_2\cdots\delta_l} \alpha_1^{\delta_1}\alpha_2^{\delta_2}\cdots\alpha_l^{\delta_l}$$

且当 $\alpha_1, \alpha_2, \cdots, \alpha_l$ 取遍它们的 $l!$ 种排列中的每一个时,f 不变。

令

$$\beta_1 = \alpha_1, \cdots, \beta_l = \alpha_l, \beta_{l+1} = \cdots = \beta_m = 0$$

$$\begin{cases} a_{\delta_1\delta_2\cdots\delta_m} = a_{\delta_1\delta_2\cdots\delta_l} & ,\delta_{l+1} = \cdots \delta_m = 0 \\ a_{\delta_1\delta_2\cdots\delta_m} = 1 & ,\text{存在某一个 } \delta_i > 0, i \geqslant l+1 \end{cases}$$

$$g = \sum_{k=0}^{n} \sum_{\delta_1+\delta_2+\cdots+\delta_m=k} a_{\delta_1\delta_2\cdots\delta_m} \beta_1^{\delta_1}\beta_2^{\delta_2}\cdots\beta_m^{\delta_m}$$

那么当 $\beta_1, \beta_2, \cdots, \beta_m$ 取遍它们的 $m!$ 种排列中的每一个时,$\alpha_1, \alpha_2, \cdots, \alpha_l$ 也取遍它们的 $l!$ 种排列中的每一个,即

$$g = \sum\nolimits_1 + \sum\nolimits_2 = \sum\nolimits_1 = \sum_{k=0}^{n} \sum_{\delta_1+\delta_2+\cdots+\delta_l=k} a_{\delta_1\delta_2\cdots\delta_l} \alpha_1^{\delta_1}\alpha_2^{\delta_2}\cdots\alpha_l^{\delta_l} = f$$

其中在 $\sum_1$ 中 $\delta_{l+1} = \cdots = \delta_m = 0$,而在 $\sum_2$ 中存在某一个 $\delta_i > 0$, $i \geqslant l+1$。

故 g 在$\beta_1,\beta_2,\cdots,\beta_m$ 取遍它们的m!种排列中的每一个时不变,由于 $g=f$,故 f 也是$\beta_1,\beta_2,\cdots,\beta_m$ 的对称函数。

引理 12.8.2 设$f(\alpha_1,\alpha_2,\cdots,\alpha_l)$是 $a\alpha_1,a\alpha_2,\cdots,a\alpha_l$ 的对称多项式,其中 a 是一个整数。$\beta_1=\alpha_1,\cdots,\beta_l=\alpha_l,\beta_{l+1}=\cdots=\beta_m=0$,那么 f 也是$a\beta_1,a\beta_2,\cdots,a\beta_m$ 的对称多项式。

证明 与引理 12.8.1 类似。

引理 12.8.3 设 $\theta_1,\theta_2,\cdots,\theta_n$ 是整系数方程 $ax^n+a_1x^{n-1}+\cdots+a_n=0$ 的 n 个根,那么 $a\theta_1,a\theta_2,\cdots,a\theta_n$ 的 n 个基本对称多项式的值都是整数。

证明 由根与系数的关系式即可得出。

引理 12.8.4 设 $f(x)=a^{lp}x^{p-1}(x-\alpha_1)^p(x-\alpha_2)^p\cdots(x-\alpha_l)^p$,那么当 $j\geqslant p-1$ 时,$f^{(j)}(x)$ 是 ax 的多项式。

证明 只须证 $f^{(p-1)}(x)$ 是 ax 的多项式即可。

$$f(x)=a^{lp}x^{p-1}(x-\alpha_1)^p(x-\alpha_2)^p\cdots(x-\alpha_l)^p=$$
$$x^{p-1}(ax-a\alpha_1)^p(ax-a\alpha_2)^p\cdots(ax-a\alpha_l)^p=x^{p-1}g^p(ax)$$

其中 $$g(u)=(u-a\alpha_1)(u-a\alpha_2)\cdots(u-a\alpha_l)$$

故由莱布尼兹公式得

$$f^{(p-1)}(x)=\sum_{k=0}^{p-1}C_{p-1}^k(g^p(ax))^{(k)}(x^{p-1})^{(p-1-k)}=$$
$$\sum_{k=0}^{p-1}C_{p-1}^k g^{p-k}(ax)a^k A_{p-1}^{p-1-k}x^k=$$
$$\sum_{k=0}^{p-1}C_{p-1}^k A_{p-1}^{p-1-k}(ax)^k g^{p-k}(ax)$$

故 $f^{(p-1)}(x)$ 已是 ax 的多项式,从而当 $j\geqslant p$ 时,$f^{(j)}(x)$ 都是 ax 的多项式。

引理 12.8.5 设 $a\alpha_1,a\alpha_2,\cdots,a\alpha_l$ 的基本对称多项式都是整数

$$f(x)=a^{lp}x^{p-1}(x-\alpha_1)^p(x-\alpha_2)^p\cdots(x-\alpha_l)^p$$

其中 p 是一个充分大的素数,那么

$$J_j=\sum_{k=1}^{l}f^{(j)}(\alpha_k)$$

是一个整数,且

(1) 当 $j<p-1$ 时,$f^{(j)}(0)$ 和 J_j 都等于 0;

(2) 当 $j=p-1$ 时,$f^{(p-1)}(0)$ 是一个非 0 整数,且$(p-1)!\mid f^{(p-1)}(0)$,但是 $p!\nmid f^{(p-1)}(0)$,$J_{p-1}=0$;

(3) 当 $j>p-1$ 或 $j\geqslant p-1$ 时,$f^{(j)}(0)$ 和 J_j 都是p!的倍数。

证明 (1) 由于0和α_k 都是$f(x)$的$p-1$重根,因此当$j<p-1$时,$f^{(j)}(0)=0$,$f^{(j)}(\alpha_k)=0$,这就证明了(1),同时也证明了当 $j<p-1$ 时,J_j 是一个整数。

由引理12.8.4知，当 $j \geqslant p-1$ 时，$f^{(j)}(x)$ 是 ax 的多项式，而 J_j 显然是 α_1，$\alpha_2,\cdots,\alpha_l$ 的对称多项式，因而也是 $a\alpha_1,a\alpha_2,\cdots,a\alpha_l$ 的对称多项式，故 $f^{(j)}(x)$ 的值是一个整数。这就证明了对任意 j，J_j 是一个整数。

(2) $$f^{(p-1)}(0)=(p-1)!a^{lp}(-1)^l(\alpha_1,\alpha_2,\cdots,\alpha_l)^p=(p-1)!(-1)^l(a\alpha_1 a\alpha_2\cdots a\alpha_l)^p$$

$a\alpha_1 a\alpha_2\cdots a\alpha_l$ 是 $a\alpha_1,a\alpha_2,\cdots,a\alpha_l$ 的基本对称多项式，由假设，它是一个与 p 无关的整数，因此当 p 充分大时，$p\nmid(a\alpha_1 a\alpha_2\cdots a\alpha_l)^p$，因而 $(p-1)!\mid f^{(p-1)}(0)$，但是 $p!\nmid f^{(p-1)}(0)$；又因为 α_k 都是 $f(x)$ 的 p 重根，所以 $f^{p-1}(\alpha_k)=0$，因而 $J_{p-1}=0$。

(3) 当 $j \geqslant p$ 时

$$f^{(j)}(x)=\sum_{k=0}^{j}C_j^k(g^p(ax))^{(k)}(x^{p-1})^{(j-k)}=\sum_{k=0}^{j}C_j^k P_j^{j-k}a^k g^{p-k}(ax)x^{p-1-j+k}=$$
$$\sum_{k=0}^{j}C_j^k P_j^{j-k}a^{j-(p-1)}g^{p-k}(ax)(ax)^{p-1-j+k}$$

由于系数中含有 j 个整数的连乘积，故上式中的每一项都是 $j!$ 的倍数，而由于 $j\geqslant p$，因而上式中的每一项都是 $p!$ 的倍数。

由此得出

$$f^{(j)}(\alpha_k)=(p!)\varphi_j(a\alpha_k)$$

其中 φ_j 是一个整系数多项式，而

$$J_j=f^{(j)}(\alpha_1)+f^{(j)}(\alpha_2)+\cdots+f^{(j)}(\alpha_l)=(p!)(\varphi_j(a\alpha_1)+\varphi_j(a\alpha_2)+\cdots+\varphi_j(a\alpha_l))$$

是 $a\alpha_1,a\alpha_2,\cdots,a\alpha_l$ 的对称多项式，因而可用 $a\alpha_1,a\alpha_2,\cdots,a\alpha_l$ 的基本对称多项式的整系数多项式表出，因而是一个整数。这就证明了当 $j\geqslant p$ 时，J_j 是 $p!$ 的倍数。

同理可证 $f^{(j)}(0)$ 是 $p!$ 的倍数。

定理 12.8.1 π 是一个超越数。

证明 假设 π 是一个代数数，那么根据定理5.4.1可知 $\theta=\pi\mathrm{i}$ 也是一个代数数，因而满足一个整系数代数方程

$$ax^n+a_1x^{n-1}+\cdots+a_n=0$$

设 $\theta_1=\theta,\theta_2,\cdots,\theta_n$ 是上面的方程的所有的根。那么由引理12.8.3可知 $a\theta_1$，$a\theta_2,\cdots,a\theta_n$ 的 n 个基本对称多项式的值都是整数。由于

$$e^{\theta_1}=e^{\pi i}=-1$$

因此 $$R=(1+e^{\theta_1})(1+e^{\theta_2})\cdots(1+e^{\theta_n})=0$$

把上式右边的括号展开，则 R 可写成 2^n 个 e^{β_i} 形式的项之和，其中

$$\beta_i=\epsilon_{i1}\theta_1+\epsilon_{i2}\theta_2+\cdots+\epsilon_{in}\theta_n$$

上式里 ϵ_{ij} 代表0或1。

假设在 β_i 中有 l 个不为 0(肯定有不为 0 的项,例如 $e^{\theta_1}, e^{\theta_2}, \cdots, e^{\theta_n}$ 就都是 $\beta_i \neq 0$ 的项,也肯定有 $\beta_i = 0$ 的项,例如展式的第一项 $1 = 1^0$ 就是 $\beta_i = 0$ 的项)。令 $q = 2^n - l$,那么

$$R = q + e^{\alpha_1} + e^{\alpha_2} + \cdots + e^{\alpha_l}$$

设 p 是充分大的素数

$$f(x) = a^{lp} x^{p-1}(x - \alpha_1)^p (x - \alpha_2)^p \cdots (x - \alpha_l)^p$$

$$I(z) = \int_0^z e^{z-u} f(u) \mathrm{d}u$$

$$\begin{aligned}
J = {} & I(\alpha_1) + I(\alpha_2) + \cdots + I(\alpha_l) = \\
& e^{\alpha_1}(f(0) + f'(0) + \cdots + f^{(s)}(0)) - (f(\alpha_1) + f'(\alpha_1) + \cdots + f^{(s)}(\alpha_1)) + \\
& e^{\alpha_2}(f(0) + f'(0) + \cdots + f^{(s)}(0)) - (f(\alpha_2) + f'(\alpha_2) + \cdots + f^{(s)}(\alpha_2)) + \cdots + \\
& e^{\alpha_l}(f(0) + f'(0) + \cdots + f^{(s)}(0)) - (f(\alpha_l) + f'(\alpha_l) + \cdots + f^{(s)}(\alpha_l)) = \\
& (e^{\alpha_1} + e^{\alpha_2} + \cdots + e^{\alpha_l})(f(0) + f'(0) + \cdots + f^{(s)}(0)) - \sum_{j=0}^{s} \sum_{k=1}^{l} f^{(j)}(\alpha_k) = \\
& -q \sum_{j=0}^{s} f^{(j)}(0) - \sum_{j=0}^{s} \sum_{k=1}^{l} f^{(j)}(\alpha_k)
\end{aligned}$$

上面式子中的 s 代表多项式 $f(x)$ 的次数。

由引理 12.8.1、引理 12.8.2、引理 12.8.3 和引理 12.8.5 知,无论对 $j < p - 1$ 还是 $j \geq p - 1$, $\sum_{k=1}^{l} f^{(j)}(\alpha_k)$ 都是 $a\alpha_1, a\alpha_2, \cdots, a\alpha_l$ 的对称多项式,因而也是 $a\beta_1, a\beta_2, \cdots, a\beta_{2^n}$ 的对称多项式。而由 β_i 的定义可知, $\sum_{k=1}^{l} f^{(j)}(\alpha_k)$ 也是 $a\theta_1, a\theta_2, \cdots, a\theta_n$ 的对称多项式。因而可由 $a\theta_1, a\theta_2, \cdots, a\theta_n$ 的初等对称多项式的整系数组合线性表出,因此是一个整数。由此看出 J 中除了 $f^{(p-1)}(0)$ 之外的项不是 0 就是 $p!$ 的倍数,故都可被 $p!$ 整除,但是 $f^{(p-1)}(0)$ 只能被 $(p-1)!$ 整除而不能被 $p!$ 整除,这就说明 $(p-1)! \mid J$ 但是 $p! \nmid J$。因而 J 是一个非 0 整数,从而 $|J| \geq (p-1)$ 或 $\left|\frac{J}{(p-1)!}\right| \geq 1$。

但是另一方面,由引理 12.7.2 知

$$|J| = \left|\sum_{k=1}^{l} I(\alpha_k)\right| \leq \sum_{k=1}^{l} |\alpha_k| e^{|\alpha_k|} f^*(|\alpha_k|) \leq c^p$$

其中 c 是一个与 p 无关的正常数,由此就得出当 p 充分大时

$$\left|\frac{J}{(p-1)!}\right| \leq \frac{c^p}{(p-1)!} \to 0$$

上式与 $\left|\frac{J}{(p-1)!}\right| \geq 1$ 矛盾,所得的矛盾就说明 π 不可能是一个代数数,从而必定是一个超越数。

第十三章 数的挑战仍在继续：几个公开问题

13.1 ζ(5),ζ(7),… 是有理数还是无理数

在第十二章12.6中，我们提到在研究个别特殊的数是否是一个无理数问题上的最新进展是法国数学家阿皮瑞(Apery)1978年在芬兰赫尔辛基举行的世界数学家大会上宣布他证明了 $\zeta(3)$ 的无理性。这一结果宣布后，一些数学家的注意力就转向了 $\zeta(5)$，$\zeta(7)$，…，一般的 $\zeta(2n+1)$ 这些数是否是无理数的问题上来。

我们知道，在证明 $\zeta(3)$ 的无理性时，$\zeta(3)$ 的积分表示式起了重要的作用。因此在研究，$\zeta(5)$，$\zeta(7)$，…，$\zeta(2n+1)$，… 的无理性时，很自然地也会先考虑他们是否有类似的积分表示式。对此我们有：

引理 13.1.1 $\zeta(n)=\int_0^1\cdots\int_0^1\int_0^1\frac{\mathrm{d}x_1\mathrm{d}x_2\cdots\mathrm{d}x_n}{1-x_1x_2\cdots x_n}$。

证明
$$\int_0^1\cdots\int_0^1\int_0^1\frac{\mathrm{d}x_1\mathrm{d}x_2\cdots\mathrm{d}x_n}{1-x_1x_2\cdots x_n}=$$
$$\int_0^1\cdots\int_0^1\int_0^1\sum_{k=0}^{\infty}x_1^kx_2^k\cdots x_n^k\mathrm{d}x_1\mathrm{d}x_2\cdots\mathrm{d}x_n=$$
$$\sum_{k=0}^{\infty}\int_0^1\cdots\int_0^1\int_0^1x_1^kx_2^k\cdots x_n^k\mathrm{d}x_1\mathrm{d}x_2\cdots\mathrm{d}x_n=$$

$$\sum_{k=0}^{\infty}\int_0^1 x_1^k\mathrm{d}x_1\int_0^1 x_2^k\mathrm{d}x_2\cdots\int_0^1 x_n^k\mathrm{d}x_n =$$

$$\sum_{k=0}^{\infty}\frac{1}{k+1}\cdot\frac{1}{k+1}\cdot\cdots\cdot\frac{1}{k+1}=\sum_{k=0}^{\infty}\frac{1}{(k+1)^n}=\sum_{k=1}^{\infty}\frac{1}{k^n}=\zeta(n)$$

引理 13.1.2 $\zeta(n+1)=-\frac{1}{n}\int_0^1\cdots\int_0^1\int_0^1\frac{\ln(x_1x_2\cdots x_n)}{1-x_1x_2\cdots x_n}\mathrm{d}x_1\mathrm{d}x_2\cdots\mathrm{d}x_n$。

证明 $\int_0^1\cdots\int_0^1\int_0^1\frac{\ln(x_1x_2\cdots x_n)}{1-x_1x_2\cdots x_n}\mathrm{d}x_1\mathrm{d}x_2\cdots\mathrm{d}x_n$

$$\int_0^1\cdots\int_0^1\int_0^1\sum_{k=0}^{\infty}x_1^kx_2^k\cdots x_n^k\ln(x_1x_2\cdots x_n)\mathrm{d}x_1\mathrm{d}x_2\cdots\mathrm{d}x_n =$$

$$\sum_{k=0}^{\infty}\int_0^1\cdots\int_0^1\int_0^1 x_1^kx_2^k\cdots x_n^k(\ln x_1+\ln x_2+\cdots+\ln x_n)\mathrm{d}x_1\mathrm{d}x_2\cdots\mathrm{d}x_n =$$

$$\sum_{k=0}^{\infty}\begin{pmatrix}\int_0^1\cdots\int_0^1\int_0^1 x_1^kx_2^k\cdots x_n^k\ln x_1\mathrm{d}x_1\mathrm{d}x_2\cdots\mathrm{d}x_n+\\ \int_0^1\cdots\int_0^1\int_0^1 x_1^kx_2^k\cdots x_n^k\ln x_2\mathrm{d}x_1\mathrm{d}x_2\cdots\mathrm{d}x_n+\cdots+\\ \int_0^1\cdots\int_0^1\int_0^1 x_1^kx_2^k\cdots x_n^k\ln x_2\mathrm{d}x_1\mathrm{d}x_2\cdots\mathrm{d}x_n\end{pmatrix}=$$

$$n\sum_{k=0}^{\infty}\int_0^1\cdots\int_0^1\int_0^1 x_1^kx_2^k\cdots x_n^k\ln x_1\mathrm{d}x_1\mathrm{d}x_2\cdots\mathrm{d}x_n =$$

$$n\sum_{k=0}^{\infty}\int_0^1 x_1^k\ln x_1\mathrm{d}x_1\int_0^1 x_2^k\mathrm{d}x_2\cdots\int_0^1 x_n^k\mathrm{d}x_n =$$

$$n\sum_{k=0}^{\infty}\frac{1}{(k+1)^{n-1}}\left(\frac{x_1^{k+1}}{k+1}\ln x_1\Big|_0^1-\frac{1}{k+1}\int_0^1 x_1^{k+1}\frac{\mathrm{d}x_1}{x_1}\right)=$$

$$-n\sum_{k=0}^{\infty}\frac{1}{(k+1)^{n+1}}=-n\sum_{k=1}^{\infty}\frac{1}{k^{n+1}}=-n\zeta(n+1)$$

由此即可得出引理。

虽然我们给出了两个形式上与 $\zeta(2),\zeta(3)$ 类似的公式，但是如果企图也从形式上模仿 $\zeta(2),\zeta(3)$ 的无理性的证明而得出 $\zeta(4),\zeta(5),\cdots$ 等数无理性的证明就会遇到一系列困难。

我们证明 $\zeta(2),\zeta(3)$ 的无理性时，第一步就是构造一个非 0 的积分 I_n，使得

$$I_n=\frac{A_n+B_n\zeta(m)}{d_n^m}$$

而构造这一积分时是很依赖于 m 的特殊性的，并没有一般的方法。目前，我们只对 $m=2,3$ 构造出了这种积分。

我们的第二步是通过积分变换和广义分部积分公式去得到一个估计，从而

可以证明当 $n \to \infty$ 时，$|bd_n^m I_n| \to 0$，由这一矛盾最后得出 $\zeta(m)$ 的无理性。

在估计积分时，我们利用了被积函数的最大值，如果按着这一路线去对 $m \geqslant 4$ 的类似积分求被积函数的最大值时，例如，我们可以得出

$$\zeta(4) = \iiiint_0^1 \frac{1 - xy}{(1 - (1 - xy)w)(1 - (1 - xy)v)} \mathrm{d}x\mathrm{d}y\mathrm{d}w\mathrm{d}v$$

而经过一系列变换后类似的被积函数为

$$\frac{x(1 - x)y(1 - y)w(1 - w)v(1 - v)(1 - xy)}{(1 - (1 - xy)w)(1 - (1 - xy)v)}$$

其在超立方体 I^4 最大值为

$$\frac{(5 - \sqrt{13})^4(-7 + 2\sqrt{13})^2}{54(-3 + \sqrt{13})^4}$$

对于 $\zeta(5)$ 类似的最大值是$\dfrac{2}{3 + \sqrt{13}}$。

然而遗憾的是，对 $\zeta(4), \zeta(5), \cdots$，我们至今无法得出一种类似于

$$I_n = \frac{A_n + B_n\zeta(m)}{d_n^m}$$

形式的积分。

13.2 欧拉常数 γ 是有理数还是无理数

在提出这一问题时，我们再次要回到调和级数

$$H_n = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$$

上来。我们早已知道，它是发散的。

我们知道

$$\int \frac{\mathrm{d}x}{1 + x} = \ln(1 + x)$$

因此调和级数可以看成是积分$\int_0^{n-1} \frac{\mathrm{d}x}{1 + x}$的近似值，因而近似于 $\ln(1 + n)$。现在我们看看，如果把两个虽然都是发散的，但很近似的量 H_n 和 $\ln(1 + n)$ 相减，会得出什么结果来？从一般的理论上来说，两个无穷大相减，既可能仍是一个无穷大，又可能趋于一个有穷的极限。我们更感兴趣于后者，因为这时我们可以得到一个渐近估计式。

引理 13.2.1 当 $n \to \infty$ 时，$H_n - \ln n$ 趋于有限极限。

证明 考虑级数

$$\sum_{n=1}^{\infty}\left(\frac{1}{n}-\ln\frac{n+1}{n}\right)$$

用微积分的知识易证

$$\ln(1+x)<x,\quad x\neq 0, x>-1$$

因此

$$\ln\frac{n+1}{n}=\ln\left(1+\frac{1}{n}\right)<\frac{1}{n}$$

另一方面，又有

$$\ln\frac{n+1}{n}=-\ln\frac{n}{n+1}=-\ln\left(1-\frac{1}{n+1}\right)>\frac{1}{n+1}$$

因而有
$$0<\frac{1}{n}-\ln\frac{n+1}{n}<\frac{1}{n}-\frac{1}{n+1}$$

再利用
$$\ln\frac{n+1}{n}=\ln(n+1)-\ln n$$

就得出

$$\begin{aligned}
0<\sum_{k=1}^{n}\left(\frac{1}{k}-\ln\frac{k+1}{k}\right)&=\sum_{k=1}^{n}\left(\frac{1}{k}-(\ln(k+1)-\ln k)\right)=\\
&1-(\ln 2-\ln 1)+\frac{1}{2}-(\ln 3-\ln 2)+\cdots+\frac{1}{n}-(\ln(n+1)-\ln n)=\\
&H_n-(\ln 2-\ln 1+\ln 3-\ln 2+\cdots+\ln(n+1)-\ln n)=\\
&H_n-(\ln(n+1)-\ln 1)=H_n-\ln(n+1)<\\
&1-\frac{1}{2}+\frac{1}{2}-\frac{1}{3}+\cdots+\frac{1}{n}-\frac{1}{n+1}=1-\frac{1}{n+1}<1
\end{aligned}$$

由此就说明正项级数 $\sum_{n=1}^{\infty}\left(\frac{1}{n}-\ln\frac{n+1}{n}\right)$ 是收敛的，因而叙列 $H_n-\ln(n+1)$ 是收敛的。又因为

$$\begin{aligned}
H_n-\ln n&=H_n-\ln(n+1)+\ln(n+1)-\ln n=\\
&H_n-\ln(n+1)+\ln\left(1+\frac{1}{n}\right)
\end{aligned}$$

故 $H_n-\ln n$ 是收敛的，这就证明了引理。

定义 13.2.1 极限 $\gamma=\lim_{n\to\infty}(H_n-\ln n)$ 称为欧拉常数。

欧拉常数 γ 和 Γ(伽马) 函数有着密切的关系，而 Γ 函数又和 B(贝塔) 函数有着密切的关系。Γ 函数和 B 函数又都称为欧拉积分。

定义 13.2.2 $\mathrm{B}(a,b)=\int_0^1 x^{a-1}(1-x)^{b-1}\mathrm{d}x\,(a>0,b>0)$ 称为第一类欧拉积分，又称为 B 函数。

引理 13.2.2 B 函数有以下性质：

(1) $\mathrm{B}(a,b)=\mathrm{B}(b,a)$；

(2)$\mathrm{B}(a,b)=\dfrac{b-1}{a+b-1}\mathrm{B}(a,b-1)$;

(3)$\mathrm{B}(a,b)=\dfrac{a-1}{a+b-1}\mathrm{B}(a-1,b)$;

(4) 设 m,n 都是自然数,则 $\mathrm{B}(m,n)=\dfrac{(m-1)!(n-1)!}{(m+n-1)!}$;

(5)$\mathrm{B}(a,b)=\int_0^{\infty}\dfrac{y^{a-1}}{(1+y)^{a+b}}\mathrm{d}y$;

(6)$\mathrm{B}(a,b)=\int_0^{1}\dfrac{x^{a-1}+x^{b-1}}{(1+x)^{a+b}}\mathrm{d}x$。

证明 (1) 在第一类欧拉积分中令 $x=1-z$ 即得。

(2) 对第一类欧拉积分做分部积分就得到

$$\begin{aligned}\mathrm{B}(a,b)&=\int_0^1 x^{a-1}(1-x)^{b-1}\mathrm{d}x=\frac{x^a(1-x)^{b-1}}{a}\Big|_0^1-\\&\frac{b-1}{a}(-1)\int_0^1 x^a(1-x)^{b-2}\mathrm{d}x=\\&\frac{b-1}{a}\int_0^1 x^{a-1}(1-x)^{b-2}\mathrm{d}x-\frac{b-1}{a}\int_0^1 x^{a-1}(1-x)^{b-1}\mathrm{d}x=\\&\frac{b-1}{a}\mathrm{B}(a,b-1)-\frac{b-1}{a}\mathrm{B}(a,b)\end{aligned}$$

由此经过整理即可得出(2)(在上面第二步中利用了恒等式 $x^a=x^{a-1}-x^{a-1}(1-x)$)。

(3) 由(1) 和(2) 即得

$$\mathrm{B}(a,b)=\mathrm{B}(b,a)=\frac{a-1}{a+b-1}\mathrm{B}(b,a-1)=\frac{a-1}{a+b-1}\mathrm{B}(a-1,b)$$

(4) 反复应用(2) 即得

$$\begin{aligned}\mathrm{B}(a,n)&=\frac{n-1}{a+n-1}\cdot\frac{n-2}{a+n-2}\cdot\cdots\cdot\frac{1}{a+1}\mathrm{B}(a,1)=\\&\frac{n-1}{a+n-1}\cdot\frac{n-2}{a+n-2}\cdot\cdots\cdot\frac{1}{a+1}\int_0^1 x^{a-1}\mathrm{d}x=\\&\frac{n-1}{a+n-1}\cdot\frac{n-2}{a+n-2}\cdot\cdots\cdot\frac{1}{a+1}\cdot\frac{1}{a}\end{aligned}$$

由此即得

$$\mathrm{B}(m,n)=\frac{(m-1)!(n-1)!}{(m+n-1)!}$$

(5) 在第一类欧拉积分中令 $x=\dfrac{y}{1+y}$ 即得

$$\mathrm{B}(a,b)=\int_0^{\infty}\frac{y^{a-1}}{(1+y)^{a+b}}\mathrm{d}y$$

(6) $$B(a,b)=\int_0^{\infty}\frac{y^{a-1}}{(1+y)^{a+b}}dy=\int_0^1\frac{y^{a-1}}{(1+y)^{a+b}}dy+\int_1^{\infty}\frac{y^{a-1}}{(1+y)^{a+b}}dy$$

在上面第二个积分中令 $y=\frac{1}{z}$,并把两个积分的变元再换回 x 就得到

$$B(a,b)=\int_0^1\frac{y^{a-1}}{(1+y)^{a+b}}dx+\int_0^1\frac{x^{b-1}}{(1+x)^{a+b}}dx=\int_0^1\frac{x^{a-1}+x^{b-1}}{(1+x)^{a+b}}dx$$

定义 13.2.3 $\Gamma(a)=\int_0^{\infty}x^{a-1}e^{-x}dx$ 称为第二类欧拉积分,又称为 Γ 函数。

引理 13.2.3 函数有以下性质;

(1)$\Gamma(1)=1$;

(2)$\Gamma(a+1)=a\Gamma(a)$;

(3)$\frac{\Gamma(a)}{t^a}=\int_0^{\infty}y^{a-1}e^{-ty}dy$;

(4)$B(a,b)=\frac{\Gamma(a)\Gamma(b)}{\Gamma(a+b)}$。

证明 (1)$\Gamma(1)=\int_0^{\infty}e^{-x}dx=-e^{x}\Big|_0^{\infty}=0-(-1)=1$。

(2) 对 $\Gamma(a)=\int_0^{\infty}x^{a-1}e^{-x}dx$ 实行分部积分即得

$$\Gamma(a+1)=\int_0^{\infty}x^a e^{-x}dx=-x^a e^{-x}\Big|_0^{\infty}+a\int_0^{\infty}x^{a-1}e^{-x}dx=a\Gamma(a)$$

(3) 在 $\Gamma(a)=\int_0^{\infty}x^{a-1}e^{-x}dx$ 中令 $x=ty(t>0)$ 得

$$\Gamma(a)=\int_0^{\infty}(ty)^{a-1}e^{-ty}t\,dy=t^a\int_0^{\infty}y^{a-1}e^{-ty}dy$$

或 $$\frac{\Gamma(a)}{t^a}=\int_0^{\infty}y^{a-1}e^{-ty}dy$$

(4) 在上面的积分中将 a 换成 $a+b$,同时将 t 换成 $t+1$(注意,这里只是在换参数,而不是在作变量替换)就得到

$$\frac{\Gamma(a+b)}{(1+t)^{a+b}}=\int_0^{\infty}y^{a+b-1}e^{-(1+t)y}dy$$

用 t^{a-1} 乘上式的两边,并从 0 到 ∞ 对 t 积分便得到

$$\Gamma(a+b)\int_0^{\infty}\frac{t^{a-1}}{(1+t)^{a+b}}dt=\int_0^{\infty}t^{a-1}dt\int_0^{\infty}y^{a+b-1}e^{-(1+t)y}dy$$

由引理 13.2.2(5) 和引理 13.2.3(3) 上面的证明知

$$\int_0^{\infty}\frac{t^{a-1}}{(1+t)^{a+b}}dt=B(a,b),\frac{\Gamma(a)}{t^a}=\int_0^{\infty}y^{a-1}e^{-ty}dy$$

因而由上式得出

$$\Gamma(a+b)\mathrm{B}(a,b)=\int_0^{\infty}y^{a+b-1}\mathrm{e}^{-y}\frac{\Gamma(a)}{t^a}\mathrm{d}y=\Gamma(a)\int_0^{\infty}y^{b-1}\mathrm{e}^{-y}\mathrm{d}y=\Gamma(a)\Gamma(b)$$

由此即可得出(3)。

引理 13.2.4

(1) $\Gamma'(a)=\int_0^{\infty}(x^{a-1}\ln x)\mathrm{e}^{-x}\mathrm{d}x$;

(2) $\Gamma'(1)=\int_0^{\infty}\mathrm{e}^{-x}\ln x\mathrm{d}x$。

证明 (1) 由于当 $x=0$ 时，积分 $\Gamma(a)=\int_0^{\infty}x^{a-1}\mathrm{e}^{-x}\mathrm{d}x$ 对于 $a\geqslant a_0>0$ 有优势函数 $x^{a_0-1}|\ln x|$，而当 $x=\infty$ 时，对于 $a\leqslant A<+\infty$ 有优势函数 $x^A\mathrm{e}^{-x}$，所以此积分对于 a 一致收敛，因而允许积分号下求导，由此即得出(1)，并且得出 $\Gamma(a)$ 本身是连续的且具有连续的微商。

(2) 在(1) 中令 $a=1$ 即得出(2)。

引理 13.2.5 Γ 函数对数的微商 $\frac{\mathrm{d}\ln\Gamma(a)}{\mathrm{d}a}=\frac{\Gamma'(a)}{\Gamma(a)}$ 有以下表达式：

(1) $\frac{\Gamma'(a)}{\Gamma(a)}=\int_0^{\infty}\left(\mathrm{e}^{-x}-\frac{1}{(1+x)^a}\right)\frac{\mathrm{d}x}{x}$（哥西公式）；

(2) $\frac{\Gamma'(a)}{\Gamma(a)}=\int_0^{\infty}\left(\frac{\mathrm{e}^{-x}}{x}-\frac{\mathrm{e}^{-ax}}{1-\mathrm{e}^{-x}}\right)\mathrm{d}x$;

(3) $\frac{\Gamma'(a)}{\Gamma(a)}+C=\int_0^1\frac{1-t^{a-1}}{1-t}\mathrm{d}t$（高斯公式），其中

$$C=-\int_0^{\infty}\left(\mathrm{e}^{-x}-\frac{1}{1+x}\right)\frac{\mathrm{d}x}{x}$$

(4) $(\ln\Gamma(a))'+C=\sum_{k=0}^{\infty}\left(\frac{1}{k+1}-\frac{1}{k+a}\right)$;

(5) $(\ln\Gamma(a))''=\sum_{k=0}^{\infty}\frac{1}{(k+a)^2}$。

证明 (1) 我们有

$$\Gamma(b)-\mathrm{B}(a,b)=\Gamma(b)-\frac{\Gamma(a)\Gamma(b)}{\Gamma(a+b)}=\frac{b\Gamma(b)}{\Gamma(a+b)}\frac{\Gamma(a+b)-\Gamma(a)}{b}=$$
$$\frac{\Gamma(b+1)}{\Gamma(a+b)}\cdot\frac{\Gamma(a+b)-\Gamma(a)}{b}$$

调换上式左右两边的位置，并令 $b\to 0$ 就得到

$$\frac{\Gamma'(a)}{\Gamma(a)}=\lim_{b\to 0}(\Gamma(b)-\mathrm{B}(a,b))=\lim_{b\to+0}\left(\int_0^{\infty}x^{b-1}\mathrm{e}^{-x}\mathrm{d}x-\int_0^{\infty}\frac{x^{b-1}}{(1+x)^{a+b}}\mathrm{d}x\right)=$$
$$\lim_{b\to+0}\int_0^{\infty}x^{b-1}\left(\mathrm{e}^{-x}-\frac{1}{(1+x)^{a+b}}\right)\mathrm{d}x$$

在 $x=0,b=0$ 附近表达式 $\frac{1}{x}\left(e^{-x}-\frac{1}{(1+x)^{a+b}}\right)$ 是 x 和 b 的连续函数，而 $x^b<1$。对于充分大的 x 和 $b\leqslant b_0$ 被积函数存在优势函数 $x^{b_0-1}\left(\frac{1}{(1+x)^a}-e^{-x}\right)$。因此我们有权利在上述积分号下取极限，由此就得到(1)。

(2) 对积分 $B(a,b)=\int_0^1 x^{a-1}(1-x)^{b-1}dx$ 做变量替换 $x=e^{-t}$，则得到

$$B(a,b)=\int_\infty^0 e^{-(a-1)t}(1-e^{-t})^{b-1}(-e^t)dt=\int_0^\infty e^{-at}(1-e^{-t})^{b-1}dt$$

由此得出

$$\frac{\Gamma'(a)}{\Gamma(a)}=\lim_{b\to 0}(\Gamma(b)-B(a,b))=$$
$$\lim_{b\to+0}\left(\int_0^\infty x^{b-1}e^{-x}dx-\int_0^\infty e^{-ax}(1-e^{-x})^{b-1}dx\right)=$$
$$\lim_{b\to+0}\left(\int_0^\infty(x^{b-1}e^{-x}-e^{-ax}(1-e^{-x})^{b-1})dx\right)$$

与(1)类似可说明积分号下取极限的合理性，由此我们就得出(2)。

(3) 设 $C=-\int_0^\infty\left(e^{-x}-\frac{1}{1+x}\right)\frac{dx}{x}$，在(1)中的公式 $\frac{\Gamma'(a)}{\Gamma(a)}=\int_0^\infty\left(e^{-x}-\frac{1}{(1+x)^a}\right)\frac{dx}{x}$ 中令 $a=1$ 就得到

$$\frac{\Gamma'(1)}{\Gamma(1)}=\Gamma'(1)=\int_0^\infty\left(e^{-x}-\frac{1}{1+x}\right)\frac{dx}{x}=-C$$

从 $\frac{\Gamma'(a)}{\Gamma(a)}=\int_0^\infty\left(e^{-x}-\frac{1}{(1+x)^a}\right)\frac{dx}{x}$ 减去上式就得出

$$\frac{\Gamma'(a)}{\Gamma(a)}+C=\int_0^\infty\left(\frac{1}{1+x}-\frac{1}{(1+x)^a}\right)\frac{dx}{x}$$

在上面的积分中再作变量替换 $t=\frac{1}{1+x}$ 就得出

$$\frac{\Gamma'(a)}{\Gamma(a)}+C=\int_1^0(t-t^a)\frac{(-dt)}{(1-t)^2}=\int_0^1\frac{1-t^{a-1}}{1-t}dt$$

(4) 在(3)中把 $\frac{1}{1-t}$ 展开成无穷等比级数就得到

$$\frac{\Gamma'(a)}{\Gamma(a)}+C=\int_0^1\frac{1-t^{a-1}}{1-t}dt=\int_0^1(1-t^{a-1})\sum_{k=0}^\infty t^k dt=\int_0^1\sum_{k=0}^\infty(t^k-t^{a+k-1})dt$$

由于被积函数存在优势级数 $(a_0+1)\sum_1^\infty\frac{1}{k^2}$，故对于 $0<a\leqslant a_0$ 一致收敛，因而可以逐项积分，由此得出

$$\frac{\Gamma'(a)}{\Gamma(a)}+C=(\ln\Gamma(a))'+C=\sum_{k=0}^\infty\left(\frac{1}{k+1}-\frac{1}{k+a}\right)$$

(5) 由于(4) 中被积函数具有优势级数$\sum_{1}^{\infty}\frac{1}{k^2}$,故(4) 对于 $a>0$ 是一致收敛的,因而允许将(4) 逐项微分,由此即得出(5)。

引理 13.2.6

(1)$\gamma=-\Gamma'(1)=\int_0^{\infty}\left(\frac{1}{1+x}-\mathrm{e}^{-x}\right)\frac{\mathrm{d}x}{x}$;

(2)$\gamma=-\int_0^1\ln(-\ln x)\mathrm{d}x$。

证明 (1) 我们在引理 13.2.5(4) 中已证明过级数$(\ln\Gamma(a))'+C=\sum_{k=0}^{\infty}\left(\frac{1}{k+1}-\frac{1}{k+a}\right)$的一致收敛性,因而允许将此级数对于 a 从 1 到 $a>0$ 逐项积分,由此即得出

$$\ln\Gamma(a)+C(a-1)=\sum_{k=0}^{\infty}\left(\frac{a-1}{k+1}-\ln\frac{k+a}{k+1}\right)$$

在上式中令 $a=2$,并注意 $\ln\Gamma(2)=\ln 1=0$ 便得出

$$C=\sum_{k=0}^{\infty}\left(\frac{1}{k+1}-\ln\frac{k+2}{k+1}\right)=\sum_{k=1}^{\infty}\left(\frac{1}{k}-\ln\frac{k+1}{k}\right)$$

由此即得出

$$C=-\Gamma'(1)=\sum_{k=1}^{\infty}\left(\frac{1}{k}-\ln\frac{k+1}{k}\right)=\lim_{n\to\infty}\sum_{k=1}^{n}\left(\frac{1}{k}-\ln\frac{k+1}{k}\right)=$$

$$\lim_{n\to\infty}\left(1+\frac{1}{2}+\cdots+\frac{1}{n}-\ln(n+1)\right)=\gamma$$

因而

$$\gamma=-\Gamma'(1)=C=\int_0^{\infty}\left(\frac{1}{1+x}-\mathrm{e}^{-x}\right)\frac{\mathrm{d}x}{x}$$

(2) 将 $\Gamma(a)=\int_0^{\infty}t^{a-1}\mathrm{e}^{-t}\mathrm{d}t$ 对 a 求导就得到

$$\Gamma'(a)=\int_0^{\infty}t^{a-1}\mathrm{e}^{-t}\ln t\mathrm{d}t$$

在上式中令 $a=1$ 即得

$$\gamma=-\Gamma'(1)=-\int_0^{\infty}\mathrm{e}^{-t}\ln t\mathrm{d}t$$

在此积分中令 $t=-\ln x$ 即得

$$\gamma=\int_1^0 x\ln(-\ln x)\left(-\frac{\mathrm{d}x}{x}\right)=-\int_0^1\ln(-\ln x)\mathrm{d}x$$

最后,再给出 γ 的一个二重积分表示。

引理 13.2.7 $\gamma=\int_0^1\int_0^1\frac{1-x}{(1-xy)(-\ln xy)}\mathrm{d}x\mathrm{d}y$。

证明 首先注意当 $0<xy<1$ 时有

$$\int_k^{\infty}(xy)^t\mathrm{d}t = \frac{(xy)^t}{\ln(xy)}\Big|_k^{\infty} = 0 - \frac{(xy)^k}{\ln(xy)} = \frac{(xy)^k}{-\ln(xy)}$$

因此

$$\int_0^1\int_0^1 \frac{1-x}{(1-xy)(-\ln xy)}\mathrm{d}x\mathrm{d}y = \int_0^1\int_0^1 \frac{(1-x)(1+xy+x^2y^2+\cdots)}{-\ln xy}\mathrm{d}x\mathrm{d}y =$$

$$\int_0^1\int_0^1 \frac{(1-x)\sum_{k=0}^{\infty}(xy)^k}{-\ln xy}\mathrm{d}x\mathrm{d}y = \sum_{k=0}^{\infty}\int_0^1\int_0^1 \frac{(1-x)(xy)^k}{-\ln xy}\mathrm{d}x\mathrm{d}y =$$

$$\sum_{k=0}^{\infty}\int_0^1\int_0^1\int_k^{\infty}(1-x)x^ty^t\mathrm{d}x\mathrm{d}y\mathrm{d}t =$$

$$\sum_{k=0}^{\infty}\int_k^{\infty}\left(\int_0^1(x^t - x^{t+1})\mathrm{d}x\int_0^1 y^t\mathrm{d}y\right)\mathrm{d}t =$$

$$\sum_{k=0}^{\infty}\int_k^{\infty}\left(\left(\frac{x^{t+1}}{t+1} - \frac{x^{t+2}}{t+2}\right)\Big|_0^1 \frac{y^{t+1}}{t+1}\Big|_0^1\right)\mathrm{d}t = \sum_{k=0}^{\infty}\int_k^{\infty}\left(\frac{1}{t+1} - \frac{1}{t+2}\right)\frac{\mathrm{d}t}{t+1} =$$

$$\sum_{k=0}^{\infty}\left(\int_k^{\infty}\frac{\mathrm{d}t}{(t+1)^2} - \int_k^{\infty}\frac{\mathrm{d}t}{(t+1)(t+2)}\right) =$$

$$\sum_{k=0}^{\infty}\left(\left(-\frac{1}{t+1}\right)\Big|_k^{\infty} - \int_k^{\infty}\left(\frac{1}{t+1} - \frac{1}{t+2}\right)\mathrm{d}t\right) =$$

$$\sum_{k=0}^{\infty}\left(\left(0+\frac{1}{k+1}\right) - \ln\frac{t+1}{t+2}\Big|_k^{\infty}\right) = \sum_{k=0}^{\infty}\left(\frac{1}{k+1} - \left(\ln 1 - \ln\frac{k+1}{k+2}\right)\right) =$$

$$\sum_{k=0}^{\infty}\left(\frac{1}{k+1} + \ln(k+1) - \ln(k+2)\right) = \sum_{k=1}^{\infty}\left(\frac{1}{k} + \ln k - \ln(k+1)\right) =$$

$$\lim_{n\to\infty}\left(\sum_{k=1}^{\infty}\left(\frac{1}{k} + \ln k - \ln(k+1)\right)\right) =$$

$$\lim_{n\to\infty}\left(1 + \frac{1}{2} + \cdots + \frac{1}{n} - \ln(n+1)\right) = \gamma$$

13.3 $3x+1$ 问题

$3x+1$ 问题也是数学中研究整数问题的一个著名的叙述起来十分简单易懂而至今尚未解决的问题。著名数学家保尔·爱尔多斯(Paul Erdös) 在谈到这一问题时曾说:"目前的数学还没有准备好去解决这种问题。"但是现在就可以看出,这一问题与 $\log_2 3$ 的有理逼近,与叙列 $\left\{\left(\frac{3}{2}\right)^k, k = 1,2,3,\cdots\right\} \pmod 1$ 的分布以及与2 adic整数 Z_2 上的遍历理论都有着密切的联系,而以上几个问题都是有着深刻理论背景的很艰深的研究领域。由此看来,虽然这个问题叙述起来

十分简单易懂而至今却尚未解决也就不奇怪了。

那么究竟什么是 $3x+1$ 问题呢?它是一个至今未有人能够证明的猜想。

$3x+1$ 猜想:任给一个自然数 x_0,然后按照迭代法则

$$x_{n+1}=T(x_n)=\begin{cases}3x_n+1, & x_n \text{ 是奇数}\\ \dfrac{x_n}{2}, & x_n \text{ 是偶数}\end{cases}$$

构造自然数的叙列 $x_0,x_1,x_2,\cdots$,那么必存在一个依赖于 x_0 的自然数 $n(x_0)$,使得 $x_{n(x_0)}=1$。

$3x+1$ 问题也称为 Callatz 问题、Syracuse 问题、角谷问题(译自日文 Kakutani)、Hasse 算法和 Ulam 问题。这个问题的确切由来现在已不清楚,只知道它曾在数学界口头流传了多年。按目前的公认看法,此问题传统上来源于德国汉堡大学的 Lothar Collatz。20 世纪 30 年代在他还是一个学生的时候,由于受兰道、佩龙和舒尔等人讲课的影响,他对数论函数发生了浓厚的兴趣,而他对图论的爱好又使他产生了将这种数论函数表示成有向图的想法。这种图的结构与迭代函数的特性有密切的联系。在他 1932 年 7 月 1 日的笔记上,他考虑了一个和 $3x+1$ 问题中的迭代类似的迭代函数 g,g 给出自然数的一个置换 P,他提出了 P 的圈的结构问题,而且特别问到这个置换中周期为 8 的圈是有限的还是无限的,即迭代 $g^{(k)}(8)$ 是否是有界的,$g(n)$ 对提出的问题现在就称为是原始的 Callatz 问题。虽然 Callatz 从未发表过他所考虑的迭代问题。但是 1950 年他在麻萨诸塞州坎布里奇市举办的国际数学家大会上传播了这些问题,并且最终导致了在数学刊物上出现了原始的 Callatz 问题。不过他所提出的原始问题从未得到回答。但是可以肯定最迟至 20 世纪 50 年代初,$3x+1$ 问题已为数学界所知,1952 年 B. Thwaites 公开叙述了这一问题,并且悬赏 1 000 英镑征求解答。

兰道(Landau, Edmund, Georg Herman, 1877—1938),德国数学家.生于柏林,卒于同地.

佩龙(Perron, Oscar, 1880—1975),德国数学家.生于弗兰肯塔尔.

舒尔(Schur, Issai, 1875—1941),犹太数学家.生于俄国莫吉廖夫,卒于现以色列特拉维夫.

在问题传播的过程中,它被赋予了各种各样的名称,由于 Callatz 的同事 H. Hasse 对此问题也颇有兴趣,并与许多人讨论了它的推广,因此它又被称为 Hasse 算法。Syracuse 问题这个名称是 Hasse20 世纪 50 年代访问 Syracuse 大学时造成的。1960 年左右 S. Kakutani 听说了这个问题并产生了兴趣,他向一部分人做了传播。他自己说:"大约有一个月的的时间,耶鲁大学几乎每个人都在研究它,但是没有结果。当我在芝加哥大学提到这个问题时发生了类似的现象。甚至由此而产生了一个笑话说是这个问题是企图延缓美国数学研究的一个阴谋计划的一部分。" 在这一过程中,这一问题又获得了角谷问题的名称。S. Ulam 也听说了这个问题,并在洛斯阿拉莫斯等地传播,所以在有些圈子里也称为 Ulam 问题。

从 1970 年以后,$3x+1$ 问题在书刊中开始以各种形式,包括作为一个以前尚未公开提出的未解决问题的形式公开传播,还有些人提供奖金悬赏解决此问

题：1970年H.S.Coxefer悬赏50美元，然后Paul Erdös是悬赏500美元，最后又有Thwaifes悬赏1 000英镑。

虽然 $3x+1$ 问题至今尚未解决，但是研究者为了解决它，还是已经提出了一些概念并获得了一些有关的结果。下面我们将选择其中一些加以介绍。但是我们强调，由于这还是一个未解决问题，因此这些介绍仅供读者参考，读者千万不要因此约束了自己的思想。

首先将 $3x+1$ 迭代所定义的映射分解为两个映射。

定义 13.3.1 设 $\mathbf{N}$ 代表全体自然数，O 代表全体正奇数，E 代表全体正偶数，定义映射 $A:O\to E, B:E\to\mathbf{N}$ 如下

$$A(n)=3n+1, n\in O, B(n)=\frac{n}{2}, n\in E$$

于是 $3x+1$ 迭代可以重新表示为

$$x_{n+1}=\begin{cases}A(x_n), & x_n\in O\\ B(x_n), & x_n\in E\end{cases}$$

$3x+1$ 问题的相空间本来是全体自然数 $\mathbf{N}$，由于任何一个正偶数经过映射 B 的足够多次的作用一定可以变成为一个正奇数，因此我们可以只限于考虑所有正奇数，也就是说，可以把 $3x+1$ 问题的相空间缩小到全体正奇数 O 上来。

定义 13.3.2 如果一个正奇数 y 是另一个正奇数 x 在映射 T 作用若干次下的结果，即

$$y=T^k(x)$$

则称 y 是一个继生数，否则称 y 是一个原生数。

引理 13.3.1 设 $O_1=\{6n-1\mid n\geqslant 1\}, O_2=\{6n+1\mid n\geqslant 1\}, O_3=\{6n-3\mid n\geqslant 1\}$，则

$$O=O_1\cup O_2\cup O_3$$

证明 显然因为一个正奇数在模6下，只能分为3个同余类就是 O_1, O_2 和 O_3。

引理 13.3.2 设 $x_1, x_2=T^k(x_1)$ 都是正奇数，$n\in\mathbf{N}, y=2^{2n}x_1+\dfrac{2^{2n}-1}{3}$，则 y 也是正奇数，且 $x_2=T^k(y)$。

证明 由于 $2^{2n}=4^n\equiv 1^n \pmod 3\equiv 1 \pmod 3$，因此 $3\mid 2^{2n}-1$。又由于3和 $2^{2n}-1$ 都是正奇数，因此 $\dfrac{2^{2n}-1}{3}$ 也是正奇数。从而 $y=2^{2n}x_1+\dfrac{2^{2n}-1}{3}$ 是正偶数加正奇数也是正奇数。

又设 $x_2=B^sA(x_1)=\dfrac{3x_1+1}{2^s}$，于是

$$3y+1=3\cdot 2^{2n}x_1+2^{2n}-1+1=3\cdot 2^{2n}x_1+2^{2n}=2^{2n}(3x_1+1)=2^{2n}\cdot 2^s x_2$$

故 $$x_2 = \frac{3y+1}{2^{2n+s}} = B^{2n+s}A(y) = T^k(y)$$

引理 13.3.3 设 $y = 2^2x + 1$,则 y 把集合 O_1, O_2, O_3 作如下变换

$$O_1 \to O_3 \to O_2 \to O_1$$

证明 由 y 和 O_1, O_2, O_3 的定义通过直接验证即可证明。

引理 13.3.4 设 s 是奇数

(1) 如果 $x_1 = \frac{3^n s - 1}{2}$ 是奇数,则 $3^{n+1}s - 1 \equiv 0 \pmod{2^t}$ $(t \geqslant 2)$,因此存在一个最大的 t 使 $x_2 = \frac{3^{n+1}s-1}{2^t}$ $(t \geqslant 2)$ 也是奇数;

(2) 如果 $x_1 = \frac{3^n s + 1}{2}$ 是奇数,则 $3^{n+1}s + 1 \equiv 0 \pmod{2^t}$ $(t \geqslant 2)$,因此存在一个最大的 t 使 $x_2 = \frac{3^{n+1}s+1}{2^t}$ $(t \geqslant 2)$ 也是奇数。

证明 (1) 设 $x_1 = \frac{3^n s - 1}{2}$ 是奇数,则

$$3^{n+1}s - 1 = 3(3^n s - 1) + 2 = 2(3x_1 + 1) = 2 \cdot 2^k x_2$$

其中 x_2 是一个奇数,k 是一个自然数。令 $t = k + 1$,则 $t \geqslant 2$,而 $x_2 = \frac{3^{n+1}s-1}{2^t}$ $(t \geqslant 2)$ 也是奇数;

(2) 设 $x_1 = \frac{3^n s + 1}{2}$ 是奇数,则

$$3^{n+1}s + 1 = 3(3^n s + 1) - 2 = 2(3x_1 - 1) = 2 \cdot 2^k x_2$$

其中 x_2 是一个奇数,k 是一个自然数。令 $t = k + 1$,则 $t \geqslant 2$,而 $x_2 = \frac{3^{n+1}s+1}{2^t}$ $(t \geqslant 2)$ 也是奇数。

引理 13.3.5

(1) 如果 $3 \cdot 2^n s - 1 = \frac{3x+1}{2}$,其中 s 是奇数,$x \in O_2 \cup O_3$,那么

$$3 \cdot 2^{n+1}s - 1 = \frac{3y+1}{2}$$

并且如果 $x \in O_2$,那么 $y \in O_3$;如果 $x \in O_3$,那么 $y \in O_2$;

(2) 如果 $3 \cdot 2^n s + 1 = \frac{3x+1}{2^2}$,其中 s 是奇数,$x \in O_1 \cup O_3$,那么

$$3 \cdot 2^{n+1}s + 1 = \frac{3y+1}{2^2}$$

并且如果 $x \in O_1$,那么 $y \in O_3$;如果 $x \in O_3$,那么 $y \in O_1$。

证明 (1) 设 $3 \cdot 2^n s - 1 = \frac{3x+1}{2}$,则 $x = 2^{n+1}s - 1$,而

$$3 \cdot 2^{n+1}s - 1 = \frac{3 \cdot 2^{n+2}s - 2}{2} = \frac{3(2^{n+2}s - 1) + 1}{2} = \frac{3y + 1}{2}$$

其中
$$y = 2^{n+2}s - 1 = 2(2^{n+1}s - 1) + 1 = 2x + 1$$

因此

$$x \in O_2 \Rightarrow x = 6t + 1 \Rightarrow y = 2x + 1 = 6(2t + 1) - 3 \in O_3$$
$$x \in O_3 \Rightarrow x = 6t - 3 \Rightarrow y = 2x + 1 = 6(2t - 1) + 1 \in O_2$$

(2) 设 $3 \cdot 2^n s + 1 = \frac{3x + 1}{2^2}$,则 $x = 2^{n+2}s + 1$,而

$$3 \cdot 2^{n+1}s + 1 = \frac{3 \cdot 2^{n+3}s + 4}{2^2} = \frac{3(2^{n+3}s + 1) + 1}{2^2} = \frac{3y + 1}{2^2}$$

其中
$$y = 2^{n+3}s + 1 = 2(2^{n+2}s + 1) - 1 = 2x - 1$$

因此

$$x \in O_1 \Rightarrow x = 6t - 1 \Rightarrow y = 2x - 1 = 6(2t) - 3 \in O_3$$
$$x \in O_3 \Rightarrow x = 6t - 3 \Rightarrow y = 2x - 1 = 6(2t - 1) - 1 \in O_1$$

引理 13.3.6 附注:如果 $3 \mid s$, $3 \cdot 2^n s - 1 = \frac{3x + 1}{2}$,则易证必有 $x \in O_1$,因此 $x \notin O_2 \cup O_3$,这就是说假定 $3 \cdot 2^n s - 1 = \frac{3x + 1}{2}$, $x \in O_2 \cup O_3$ 蕴含条件 $3 \nmid s$。

同样,如果 $3 \mid s$, $3 \cdot 2^n s + 1 = \frac{3x + 1}{2^2}$,则易证必有 $x \in O_2$,因此 $x \notin O_1 \cup O_3$,这就是说假定 $3 \cdot 2^n s + 1 = \frac{3x + 1}{2^2}$, $x \in O_1 \cup O_3$ 蕴含条件 $3 \nmid s$。

引理 13.3.7

(1) 设 $x \in O_1 \cup O_2$,则存在无穷多个奇数 x_1 使得

$$x \in Orbit(x_1) = \{T^n(x_1) \mid n = 0, 1, 2, \cdots\}$$

(2) 设 $x \in O_3$,则不存在任何奇数 x_1 使得

$$x \in Orbit(x_1) = \{T^n(x_1) \mid n = 0, 1, 2, \cdots\}$$

证明 (1) 设 $x \in O_1$,则 $x = 6m - 1$,于是 $x = \frac{3x_2 + 1}{2}$,其中 $x_2 = 4m - 1$。由引理 13.3.2 知存在无穷多个奇数

$$x_1 = y_n = 2^{2n}x_2 + \frac{2^{2n} - 1}{3}$$

使得 $x = T^k(y_n)$,即

$$x \in Orbit(y_n) = Orbit(x_1)$$

如果 $x \in O_2$,则 $x = 6m + 1$,于是 $x = \frac{3x_2 + 1}{2^2}$,其中 $x_2 = 8m + 1$。由引理 13.3.2 知存在无穷多个奇数

$$x_1 = y_n = 2^{2n}x_2 + \frac{2^{2n}-1}{3}$$

使得 $x = T^k(y_n)$，即

$$x \in Orbit(y_n) = Orbit(x_1)$$

(2) 设 $x \in O_3$，且存在奇数 x_1 使得 $x \in Orbit(x_1)$，那么必存在 $y \in Orbit(x_1)$ 而 $x = \frac{3y+1}{2^t}$，于是

$$3y + 1 = 2^t x = 2^t(6m - 3)$$

由于此式左边被3除余1，而右边可以被3整除，因而不可能成立。这就得出矛盾，所得的矛盾就说明不可能存在任何奇数 x_1 使得 $x \in Orbit(x_1)$。

引理 13.3.8 x 是一个原生数的充分必要条件是 $x \in O_3$ 或者 $x \equiv 3(\mathrm{mod}\ 6)$。

证明 由引理 13.3.7(2) 即知充分性成立。

必要性：设是原生数。如果 $x \notin O_3$，那么 $x \in O_1 \cup O_2$。于是由引理 13.3.7(1) 知存在奇数 x_1 使得 $x \in Orbit(x_1)$。这说明 x 不是原生数，因而与假设矛盾，所得的矛盾就说明必有 $x \in O_3$。这就证明了必要性。

由上述引理易证 $3x+1$ 猜想只要对全体原生数成立，那么它就对全体自然数成立。也就是说，我们可以把 $3x+1$ 问题的相空间缩小到全体原生数上即数类 O_3 上。

上面，我们集中讨论了 $3x+1$ 问题的相空间，下面我们给出映射 T 的一些性质，和 $3x+1$ 问题的一些等价命题。

定义 13.3.3 设 x_1 是一个正奇数，如果存在自然数 k，使得 $T^k(x_1) = 1$。则称

$$n = \min\{k \mid T^k(x_1) = 1\}$$

为 x_1 的停止时间，称 $M = \max\{T^k(x_1) \mid 0 \leqslant k \leqslant n\}$ 为 $Orbit(x_1)$ 的最高峰。

定义 13.3.4 称 $\{1,4,2\}$ 是映射 T 的平凡周期解。

易于证明：

引理 13.3.9 $3x+1$ 猜想等价于对于任何正奇数 x_1

(1) x_1 的停止时间是有限的；

(2)(i) $Orbit(x_1)$ 的最高峰是有限的或 $Orbit(x_1)$ 是有界的；并且

(ii) 除了平凡周期解外，映射 T 不存在任何周期解。

虽然 $3x+1$ 猜想成立的一个必要条件是 $Orbit(x_1)$ 是有界的，但是我们可以证明：

引理 13.3.10 设 $x = 2^n y - 1$ 是一个奇数，其中 y 是一个奇数。那么 $T^{2j}(x) = 3^j 2^{n-j} y - 1, 0 \leqslant j \leqslant n$，因而 $T^{2n}(x) = 3^n y - 1$，因而映射 T 不存在对所有奇数

都成立的一致的界。

证明 由数学归纳法即可证明。

引理 13.3.11 设 h 是一个自然数，$C = BA$，因而 $C(x) = \frac{3x+1}{2}$，那么

$$C^h(x) = \left(\frac{3}{2}\right)^h (x+1) - 1$$

证明 用数学归纳法即可证明。

引理 13.3.12 设是一个正奇数，$x_1 = x, x_2 = T(x_1), \cdots, x_m = T(x_{m-1})$，那么必存在自然数 $h_1, k_1, h_2, k_2, \cdots, h_n, k_n$ 使得

$$x_m = C^{h_n}B^{k_{n-1}}C^{h_{n-1}}\cdots B^{k_1}C^{h_1}(x)$$

或

$$x_m = B^{k_n}C^{h_n}B^{k_{n-1}}C^{h_{n-1}}\cdots B^{k_1}C^{h_1}(x)$$

证明 由映射 A，B 和 C 的意义即可得出。

定义 13.3.5 映射 $g: O \to O$ 的意义为 $g(x) = B^kC^h(x)$。其中 x 是一个奇数，$C^h(x)$ 是偶数，$g(x)$ 又是一个奇数。

引理 13.3.13 设 $x_2 = g(x_1), x_3 = g(x_2), \cdots, x_n = g(x_{n-1})\cdots$ 那么

$$x_1 = 2^{h_1}y_1 - 1, 3^{h_1}y_1 - 1 = 2^{k_1}x_2$$

$$x_2 = 2^{h_2}y_2 - 1, 3^{h_2}y_2 - 1 = 2^{k_2}x_3$$

$$\vdots$$

$$x_n = 2^{h_n}y_n - 1, 3^{h_n}y_n - 1 = 2^{k_n}x_{n+1}$$

$$\vdots$$

其中 $x_1, x_2, \cdots, x_n, \cdots, y_1, y_2, \cdots, y_n, \cdots$ 都是奇数，$h_1, k_1, h_2, k_2, \cdots, h_n, k_n, \cdots$ 都是自然数。

证明 由引理 13.3.11 即得。

从上面这个引理就可看出，在 $3x+1$ 问题的迭代过程中，连续的出现以 2 为底的幂和以 3 为底的幂的表示形式之间的交换。因此 $3x+1$ 猜想的谜底必定和 2 的幂和 3 的幂之间的比例有关，而且一定有什么因素在此互相转换的过程中被消耗殆尽，以至于这种转换过程不能无限地进行下去。但是到底是什么具体的因素，我们现在还不得而知，仍然没有认识到。

这种转换过程的复杂性可以从下面的例子中看出来。就是如果你从 1 开始，连续不断地用相邻的奇数作初值就会发现从 1 到 25 的停止时间都不长，但是到了 27 停止时间却突然变长，具体的数据是 $g^{17}(27) = 1$，停止时间，$n = 111$，$\max Orbit(27) = 3\,077$。如果你继续试验下去，就会发现，每过一段数，停止时间就会突然加长，出现一个高峰，然而此高峰出现的规律又极其复杂，很难用一些常见的初等函数模拟。比如说，既然 $3x+1$ 猜想的谜底必定和 2 的幂与 3 的幂之间的比例有关，因此你认为应该用 3 与 2 的比例的幂的对数来表达高峰出

现的规律，那显然不对，因为 $\ln\left(\frac{3}{2}\right)^n$ 是一个单调的函数，这里 n 是用来充当初值的奇数。我认为正确的思想是从 $\left(\frac{3}{2}\right)^n$ 中分出 $\left(\frac{3}{2}\right)^k$ 的成分，这里 $\left(\frac{3}{2}\right)^k$ 是一个十分接近于整数的数，把它扔掉后，剩余的部分才可能出现一阵一阵的高峰。但是如何具体实现这一思想，并比较准确地与实际的数据拟合还不知道。

另外在 $Orbit(n)$ 中达到最高峰的方式和规律也是很复杂的，它不是简单的先增高，到达最高峰后再减小，呈现出一个单峰函数的式样，而是振动式的到达最高峰，然后又振动式地降到 1，所以这个规律就显得十分复杂。例如在 $Orbit(27)$ 中，在 27 之后，先是上升到 41，然而又下降到 31，然后再上升到 47，71，107，161，之后又开始下降到 121，91，又开始上升 … 这个 27 是个很好的例子，任何高超的理论都要接受它的检验，我看到过一些长篇的文章、理论和定理一大套，但是都不能满意地解释 27 的行为。

引理 13.3.14 $3x+1$ 迭代的 $B^kC(x)=x$ 形的周期解只有唯一解 $k=x=1$，即平凡周期解，其中 x 是一个正奇数。

证明 由引理 13.3.11 和 $B^kC(x)=x$ 得出

$$\frac{\frac{3}{2}(x+1)-1}{2^k}=x$$

由此得出

$$\frac{3}{2}(x+1)-1=2^kx,3x+3-2=2^{k+1}x,(2^{k+1}-3)x=1$$

因而必有 $x=1,2^{k+1}-3=1$ 或 $k=x=1$。

定义 13.3.6 设 n 是一个自然数，k_n 的意义是满足不等式

$$2^{n+k_n}<3^n<2^{n+k_n+1}$$

的唯一自然数；

$$u_n=3^n-2^{n+k_n}$$

$$\alpha_n=2^{n+k_n},\beta_n=2^{k_n}$$

引理 13.3.15

(1) $0<u_n<\alpha_n$；

(2) $3u_n\neq\alpha_n$；

(3) $2^{n+1+k_n}<3^{n+1}<2^{n+1+k_n+2}$。

证明 (1) 由 k_n 的定义(定义 13.3.6) 知 $2^{n+k_n}<3^n<2^{n+k_n+1}$，因此

$$0<u_n<2^{n+k_n+1}-2^{n+k_n}=2^{n+k_n}=\alpha_n$$

(2) 如果 $3u_n=\alpha_n=2^{n+k_n}$，那么必有

$$3^{n+1}=3\cdot3^n=3(u_n+\alpha_n)=3u_n+3\alpha_n=4\alpha_n=2^{n+k_n+2}$$

因为上式左边是 3 的幂，而右边是 2 的幂，因此这是不可能的。所得的矛盾就说明了 $3u_n \neq a_n$。

(3) 由 k_n 的定义(定义 13.3.6) 知 $2^{n+k_n} < 3^n < 2^{n+k_n+1}$，因此

$$2^{n+1+k_n} = 2 \cdot 2^{n+k_n} < 3 \cdot 3^n = 3^{n+1} < 3 \cdot 2^{n+k_n+1} < 4 \cdot 2^{n+k_n+1} = 2^{n+1+k_n+2}$$

引理 13.3.16 在下面的两组命题中，每组中的 4 个命题都是互相等价的。

(1.1)$3u_{n-1} < a_{n-1} \Leftrightarrow$(1.2)$k_n = k_{n-1} \Leftrightarrow$(1.3)$u_n = 3u_{n-1} + a_{n-1} \Leftrightarrow$(1.4)$a_n = 4a_{n-1}$；

(2.1)$3u_{n-1} > a_{n-1} \Leftrightarrow$(2.2)$k_n = k_{n-1} + 1 \Leftrightarrow$(2.3)$u_n = 3u_{n-1} - a_n \Leftrightarrow$(2.4)$a_n = 2a_{n-1}$。

证明 (1) 我们首先证明(1.1)$\Rightarrow$(1.2) 以及(2.1)$\Rightarrow$(2.2)。

假设 $3u_{n-1} < a_{n-1}$，那么

$$3u_{n-1} = 3(3^{n-1} - a_{n-1}) = 3^n - 3a_{n-1}$$

因此由引理 13.3.14，就有

$$3u_{n-1} > 2^{n+k_{n-1}} - 3 \cdot 2^{n-1+k_{n-1}}$$

或

$$2^{n+k_{n-1}} < 3 \cdot 2^{n+k_{n-1}} + 3u_{n-1}$$

同时根据假设又有

$$3 \cdot 2^{n-1+k_{n-1}} + 3u_{n-1} < 3 \cdot 2^{n-1+k_{n-1}} + 2^{n-1+k_{n-1}} = 4 \cdot 2^{n-1+k_{n-1}} = 2^{n+k_{n-1}+1}$$

故

$$2^{n+k_{n-1}} < 3 \cdot 2^{n+k_{n-1}} + 3u_{n-1} < 2^{n+k_{n-1}+1}$$

或者

$$2^{n+k_{n-1}} < 3^n < 2^{n+k_{n-1}+1}$$

因而根据 k_n 的意义就有

$$k_n = k_{n-1}$$

这就证明了(1.1)$\Rightarrow$(1.2)；

如果 $3u_{n-1} > a_{n-1}$，那么

$$3 \cdot 2^{n-1+k_{n-1}} + 3u_{n-1} > 3 \cdot 2^{n-1+k_{n-1}} + 2^{n-1+k_{n-1}} > 4 \cdot 2^{n-1+k_{n-1}} = 2^{n+k_{n-1}+1}$$

同时根据引理 13.3.15(3) 又有

$$3 \cdot 2^{n-1+k_{n-1}} + 3u_{n-1} = 3(2^{n-1+k_{n-1}} + u_{n-1}) = 3 \cdot 3^{n-1} = 3^n < 2^{n-1+k_{n-1}+2}$$

因而

$$2^{n-1+k_{n-1}+1} < 3 \cdot 2^{n-1+k_{n-1}} + 3u_{n-1} < 2^{n-1+k_{n-1}+2}$$

或

$$2^{n-1+k_{n-1}+1} < 3^n < 2^{n-1+k_{n-1}+1+1}$$

因而根据 k_n 的意义就有

$$k_n = k_{n-1} + 1$$

这就证明了(2.1)$\Rightarrow$(2.2)。

(2) 下面我们再证明(1.2)$\Rightarrow$(1.1) 以及(2.2)$\Rightarrow$(2.1)。

设 $k_n = k_{n-1}$，如果 $3u_{n-1} \geqslant a_{n-1}$，那么由引理 13.3.15(2) 知 $3u_{n-1} \neq a_{n-1}$，因此必有 $3u_{n-1} > a_{n-1}$，再由(1) 已证可知 $k_n = k_{n-1} + 1$。这与 $k_n = k_{n-1}$ 矛盾，因此只能有 $3u_{n-1} < a_{n-1}$。

这就证明了(1.2)⇒(1.1),同理可证(2.2)⇒(2.1)。

(3) 现在我们证明(1.2)⇒(1.3)⇒(1.4) 以及(2.2)⇒(2.3)⇒(2.4)。

设 $k_n = k_{n-1}$,这时

$$u_n = 3^n - 2^{n+k_n} = 3 \cdot 3^{n-1} - 2^{n+k_n} = 3(2^{n-1+k_{n-1}} + u_{n-1}) - 2^{n+k_n} = 3 \cdot 2^{n-1+k_{n-1}} + 3u_{n-1} - 2^{n+k_{n-1}} = 3u_{n-1} + 3 \cdot 2^{n-1+k_{n-1}} - 2 \cdot 2^{n-1+k_{n-1}} = 3u_{n-1} + \alpha_{n-1}$$

并且

$$\alpha_n = 3^n - u_n = 3 \cdot 3^{n-1} - u_n = 3(u_{n-1} + \alpha_{n-1}) - (3u_{n-1} + \alpha_{n-1}) = 2\alpha_{n-1}$$

这就证明了(1.2)⇒(1.3)⇒(1.4)。

设 $k_n = k_{n-1} + 1$,这时

$$u_n = 3^n - 2^{n+k_n} = 3 \cdot 3^{n-1} - 2^{n+k_{n-1}+1} = 3(2^{n-1+k_{n-1}} + u_{n-1}) - 2^{n-1+2+k_{n-1}} = 3 \cdot 2^{n-1+k_{n-1}} + 3u_{n-1} - 2^{n-1+2+k_{n-1}} = 3u_{n-1} + 3 \cdot 2^{n-1+k_{n-1}} - 4 \cdot 2^{n-1+k_{n-1}} = 3u_{n-1} - \alpha_{n-1}$$

并且

$$\alpha_n = 3^n - u_n = 3 \cdot 3^{n-1} - u_n = 3(u_{n-1} + \alpha_{n-1}) - (3u_{n-1} - \alpha_{n-1}) = 4\alpha_{n-1}$$

这就证明了(2.2)⇒(2.3)⇒(2.4)。

(4) 最后,与(2) 类似我们可证明(1.3)⇒(1.1),(2.3)⇒(2.1) 以及(1.4)⇒(1.1),(2.4)⇒(2.1)。

这就证明了引理。

引理 13.3.17

(1) 如果 $k_{n+1} = k_n$,则 $k_{n+2} = k_{n+1} + 1$;

(2) 如果 $k_{n+1} = k_n + 1, k_{n+2} = k_{n+1} + 1$,则 $k_{n+3} = k_{n+2}$。

证明 由引理 13.3.17 得

(1) 如果 $k_{n+1} = k_n$,则 $3u_n < \alpha_n, u_{n+1} = 3u_n + \alpha_n$,因而

$$3u_{n+1} = 9u_n + 3\alpha_n > 2\alpha_n = 2 \cdot 2^{n+k_n} = 2^{n+1+k_{n+1}} = \alpha_{n+1}$$

故
$$k_{n+2} = k_{n+1} + 1$$

(2) 如果 $k_{n+1} = k_n + 1, k_{n+2} = k_{n+1} + 1$,则 $k_{n+2} = k_n + 2, 3u_n > \alpha_n, 3u_{n+1} > \alpha_{n+1}$,因而

$$u_{n+1} = 3u_n - \alpha_n$$

$$u_{n+2} = 3u_{n+1} - \alpha_{n+1} = 3(3u_n - \alpha_n) - \alpha_{n+1} = 9u_n - 3\alpha_n - \alpha_{n+1} = 9u_n - 3 \cdot 2^{n+k_n} - 2^{n+1+k_{n+1}} = 9u_n - 3 \cdot 2^{n+k_n} - 2^{n+1+k_n+1} = 9u_n - 3 \cdot 2^{n+k_n} - 4 \cdot 2^{n+k_n} = 9u_n - 7 \cdot 2^{n+k_n} = 9u_n - 7\alpha_n$$

$$3u_{n+2} = 27u_n - 21\alpha_n < 27\alpha_n - 21\alpha_n < 16\alpha_n = 2^{n+2+k_n+2} = 2^{n+2+k_{n+2}} = \alpha_{n+2}$$

由此即得
$$k_{n+3} = k_{n+2}$$

引理 13.3.18 设

$$\{\underline{k}_n\} = 0,1,1,2,2,3,3,4,4,5,5,6,6,\cdots$$

$$\{\bar{k}_n\} = 0,1,1,2,\{2,3,4\},\{4,5,6\},\{6,7,8\},\{8,9,10\},\cdots$$

则

$$\underline{k}_n \leqslant k_n \leqslant \bar{k}_n$$

证明 由引理 13.3.18 可知如果 $k_{n+1} = k_n$，则 $k_{n+2} = k_{n+1} + 1$；同时如果 $k_{n+1} = k_n + 1$，$k_{n+2} = k_{n+1} + 1$，则 $k_{n+3} = k_{n+2}$。这就是说，在叙列$\{k_n\}$如果有两个相邻的项相等，那么这两项后面的一项必定要增加 1，而如果在两个相邻的项中，每一个都比前一项增加 1，那么这两项后面的一项必定不能再增加。

再由 $k_1 = 0$，$k_2 = 1$，$k_3 = 1$，$k_4 = 2$，即可得出引理。

引理 13.3.19 如果

$$u_n = 3u_{n-1} - \alpha_{n-1}$$

$$u_{n+1} = 3u_n - \alpha_n$$

$$u_{n+2} = 3u_{n+1} + \alpha_{n+1}$$

则

$$u_{n+3} = 3u_{n+2} - \alpha_{n+2}$$

$$u_{n+4} = 3u_{n+3} + \alpha_{n+3}$$

证明 由已知条件和引理 13.3.16 得出

$$3u_{n-1} > \alpha_{n-1}, 3u_n > \alpha_n, 3u_{n+1} < \alpha_{n+1}$$

$$\alpha_n = 4\alpha_{n-1}, \alpha_{n+1} = 4\alpha_n, \alpha_{n+2} = 2\alpha_{n+1}$$

因而 $$3u_{n+2} = 3(3u_{n+1} + \alpha_{n+1}) = 9u_{n+1} + 3\alpha_{n+1} > 2\alpha_{n+1} = \alpha_{n+2}$$

故 $$u_{n+3} = 3u_{n+2} - \alpha_{n+2}, \alpha_{n+3} = 4\alpha_{n+2}$$

同理

$$3u_{n+3} = 3(3u_{n+2} - \alpha_{n+2}) = 3^2u_{n+2} - 3\alpha_{n+2} = 3^2(3u_{n+1} + \alpha_{n+1}) - 6\alpha_{n+1} = \cdots =$$
$$3^5u_{n-1} - 141\alpha_{n-1} = 3^5(3^{n-1} - \alpha_{n-1}) - 141\alpha_{n-1} = 3^5 \cdot 3^{n-1} - 384\alpha_{n-1}$$

由 k_n 和α_n 的定义可知$\alpha_{n-1} = 2^{n-1+k_{n-1}}$，而$3^{n-1} < 2^{n-1+k_{n-1}+1} = 2\alpha_{n-1}$，因而上式小于

$$3^5 \cdot 2\alpha_{n-1} - 384\alpha_{n-1} < 128\alpha_{n-1} = \alpha_{n+3}$$

故 $$u_{n+4} = 3u_{n+3} + \alpha_{n+3}, \alpha_{n+4} = 2\alpha_{n+3}$$

引理 13.3.20 如果

$$u_n = 3u_{n-1} + \alpha_{n-1}$$

$$u_{n+1} = 3u_n - \alpha_n$$

$$u_{n+2} = 3u_{n+1} + \alpha_{n+1}$$

$$u_{n+3} = 3u_{n+2} - \alpha_{n+2}$$

$$u_{n+4} = 3u_{n+3} + \alpha_{n+3}$$

则

$$u_{n+5}=3u_{n+4}-a_{n+4}$$
$$u_{n+6}=3u_{n+5}-a_{n+5}$$

证明　由假设及引理 13.3.16 可以计算出

$$a_n=2a_{n-1},a_{n+1}=4a_n,a_{n+2}=2a_{n+1},a_{n+3}=4a_{n+2},a_{n+4}=2a_{n+3}$$

因而 $$3u_{n+4}=3(3u_{n+3}+a_{n+3})>3a_{n+3}>2a_{n+3}=a_{n+4}$$

故 $$u_{n+5}=3u_{n+4}-a_{n+4},a_{n+5}=4a_{n+4}$$

$$3u_{n+5}=3(u_{n+4}-a_{n+4})=3^2u_{n+4}-3a_{n+4}=3^2(3u_{n+3}+a_{n+3})-6a_{n+3}=$$
$$3^3u_{n+3}+3a_{n+3}=\cdots=3^7u_{n-1}+651a_{n-1}>512a_{n-1}>a_{n+5}$$

因而 $$u_{n+6}=3u_{n+5}-a_{n+5}$$

引理 13.3.21　如果

$$u_n=3u_{n-1}+a_{n-1}$$
$$u_{n+1}=3u_n-a_n$$
$$u_{n+2}=3u_{n+1}+a_{n+1}$$
$$u_{n+3}=3u_{n+2}-a_{n+2}$$
$$u_{n+4}=3u_{n+3}+a_{n+3}$$

则

$$u_{n+5}=3u_{n+4}-a_{n+4}$$
$$u_{n+6}=3u_{n+5}-a_{n+5}$$
$$u_{n+7}=3u_{n+6}+a_{n+6}$$
$$u_{n+8}=3u_{n+7}-a_{n+7}$$
$$u_{n+9}=3u_{n+8}+a_{n+8}$$
$$u_{n+10}=3u_{n+9}-a_{n+9}$$
$$u_{n+11}=3u_{n+10}-a_{n+10}$$

证明　由已知条件和引理 13.3.16 得出

$$3u_{n-1}<a_{n-1},3u_n>a_n,3u_{n+1}<a_{n+1},3u_{n+2}>a_{n+2},3u_{n+3}<a_{n+3}$$
$$a_n=2a_{n-1},a_{n+1}=4a_n,a_{n+2}=2a_{n+1},a_{n+3}=4a_{n+2},a_{n+4}=2a_{n+3}$$
$$u_{n+5}=3u_{n+4}-a_{n+4},u_{n+6}=3u_{n+5}-a_{n+5},3u_{n+4}>a_{n+4},3u_{n+5}>a_{n+5}$$
$$a_{n+5}=4a_{n+4},a_{n+6}=4a_{n+5}$$

因此

$$3u_{n+6}=3(3u_{n+5}-a_{n+5})=9u_{n+5}-3a_{n+5}=9(3u_{n+4}-a_{n+4})-12a_{n+4}=$$
$$27u_{n+4}-21a_{n+4}=27(3^{n+4}-a_{n+4})-21a_{n+4}=27\cdot 3^{n+4}-48a_{n+4}<$$
$$27\cdot 2a_{n+4}-48a_{n+4}<16a_{n+4}=a_{n+6}$$

故
$$u_{n+7}=3u_6+\alpha_{n+6},\alpha_{n+7}=2\alpha_{n+6}$$
$$3u_{n+7}=3(3u_{n+6}+\alpha_{n+6})=9u_{n+6}+3\alpha_{n+6}>2\alpha_{n+6}=\alpha_{n+7}$$
故
$$u_{n+8}=3u_{n+7}-\alpha_{n+7},\alpha_{n+8}=4\alpha_{n+7}=8\alpha_{n+6}$$
$$3u_{n+8}=3(3u_{n+7}-\alpha_{n+7})=9u_{n+7}-3\alpha_{n+7}=9(3u_{n+6}+\alpha_{n+6})-6\alpha_{n+6}=$$
$$27u_{n+6}+3\alpha_{n+6}<8\alpha_{n+6}=\alpha_{n+8}$$
故
$$u_{n+9}=3u_{n+8}+\alpha_{n+8},\alpha_{n+9}=2\alpha_{n+8}$$
$$3u_{n+9}=3(3u_{n+8}+\alpha_{n+8})=9u_{n+8}+3\alpha_{n+8}>2\alpha_{n+8}=\alpha_{n+9}$$
故
$$u_{n+10}=3u_{n+9}-\alpha_{n+9},\alpha_{n+10}=4\alpha_{n+9}$$
应用引理 13.3.20 中 $u_{n+6}=3u_{n+5}-\alpha_{n+5}$ 的证明过程中的
$$3u_{n+5}=3^7u_{n-1}+651\alpha_{n-1}$$
$$3u_{n+10}=3(3u_{n+9}-\alpha_{n+9})=3^2u_{n+9}-3\alpha_{n+9}=3^2(3u_{n+8}+\alpha_{n+8})-6\alpha_{n+8}=\cdots=$$
$$3^6u_{n+5}-39\alpha_{n+5}=3^5\cdot 3u_{n+5}-39\alpha_{n+5}=$$
$$3^5(3^7u_{n-1}+651\alpha_{n-1})-39\cdot 512\alpha_{n-1}=$$
$$3^{12}u_{n-1}+156\ 657\alpha_{n-1}>131\ 072\alpha_{n-1}=\alpha_{n+10}$$
故
$$u_{n+11}=3u_{n+10}-\alpha_{n+10},\alpha_{n+11}=4\alpha_{n+10}$$
由上面的证明可知如果 $u_n=3u_{n-1}+\alpha_{n-1}$,那么由引理 13.3.17 知必定有 $u_{n+1}=3u_n-\alpha_n$,同时由实际数据可知,如果 $u_n=3u_{n-1}-\alpha_{n-1}$,那么 $u_{n+1}=3u_n-\alpha_n$ 和 $u_{n+1}=3u_n+\alpha_n$ 这两种情况都可能发生,然而如果 $u_n=3u_{n-1}-\alpha_{n-1}$, $u_{n+1}-3u_n-\alpha_n$,那么必定有 $u_{n+2}=3u_{n+1}-\alpha_{n+1}$。形象地说就是在连续几个迭代式中,对于迭代右边的符号有以下规律:加号后面必定跟着减号,减号后面可以跟着减号,也可以跟着加号,但是两个减号之后必定跟着加号。或者也可以反过来说,加号之前必定是减号,减号之前可以是加号也可以是减号。

由此可知,在这种情况下必然有
$$u_{n-1}=3u_{n-2}-\alpha_{n-2},\alpha_{n-1}=4\alpha_{n-2},\beta_{n-1}=2\beta_{n-2}$$
$$u_{n-2}=3u_{n-3}-\alpha_{n-3},\alpha_{n-2}=4\alpha_{n-3},\beta_{n-2}=2\beta_{n-3}$$
我们把这种情况简记为(-,-,+)。

利用这种记法,我们可以把引理 13.3.19、13.2.20 和 13.3.21 简单地叙述成:

引理 13.3.19 (-,-,+)⇒(-,-,+,-,+);

引理 13.3.20 (+,-,+,-,+)⇒(+,-,+,-,+,-,-);

引理 13.3.21 (+,-,+,-,+,-,-)⇒(+,-,+,-,+,-,-,+,-,+,-,-)。

引理 13.3.22 设 $\alpha_n=2^{n+k_n},\beta_n=2^{k_n}$,那么

(1) 当 $n=1$ 时,$u_1=\alpha_1-2\beta_1+1=1$;

(2) 当 $2\leqslant n\leqslant 5$ 时,$u_n<\alpha_n-2\beta_n+1$;

(3) 当 $n \geqslant 6$ 时，$u_n < \frac{7}{11}(\alpha_n - 2\beta_n + 1)$。

因而对任何自然数 $n > 1$ 都成立 $u_n < \alpha_n - 2\beta_n + 1$。

证明 (1)(2) 由直接验证即可得出。

对 $n = 6,7$，可直接验证引理成立。

(3) 如果 $u_n = 3u_{n-1} + \alpha_{n-1}$，那么 $\alpha_n = 2\alpha_{n-1}, \beta_n = \beta_{n-1}$，并且由上面所说的迭代规律可知

$$u_{n-1} = 3u_{n-2} - \alpha_{n-2}, \alpha_{n-1} = 4\alpha_{n-2}, \beta_{n-1} = 2\beta_{n-2}$$

因此 $\quad u_n = 3u_{n-1} + \alpha_{n-1} = 3(3u_{n-2} - \alpha_{n-2}) + 4\alpha_{n-2} = 9u_{n-2} + \alpha_{n-2}$

由归纳法假设有

$$u_{n-2} < \frac{7}{11}(\alpha_{n-2} - 2\beta_{n-2} + 1)$$

因而
$$u_n < \frac{63}{11}(\alpha_{n-2} - 2\beta_{n-2} + 1) + \alpha_{n-2} \leqslant \frac{74}{11}\alpha_{n-2} - \frac{126}{11}\beta_{n-2} + \frac{63}{11} \leqslant \frac{74}{88}\alpha_n - \frac{63}{11}\beta_n + \frac{63}{11} < \frac{7}{11}(\alpha_n - 2\beta_n + 1) - \frac{49}{11}\left(\beta_n - \frac{9}{7}\right) < \frac{7}{11}(\alpha_n - 2\beta_n + 1)$$

（由于当 $n \geqslant 2$ 时，$\beta_n \geqslant 2 > \frac{9}{7}$）

如果 $u_n = 3u_{n-1} - \alpha_{n-1}$，那么 $\alpha_n = 4\alpha_{n-1}, \beta_n = 2\beta_{n-1}$。由归纳法假设有

$$u_{n-1} < \frac{7}{11}(\alpha_{n-1} - 2\beta_{n-1} + 1)$$

因而
$$u_n < \frac{21}{11}(\alpha_{n-1} - 2\beta_{n-1} + 1) - \alpha_{n-1} \leqslant \frac{10}{11}\alpha_{n-1} - \frac{42}{11}\beta_{n-1} + \frac{21}{11} \leqslant \frac{5}{22}\alpha_n - \frac{21}{11}\beta_n + \frac{21}{11} < \frac{5}{11}(\alpha_n - 2\beta_n + 1) - \left(\beta_n - \frac{16}{11}\right) < \frac{5}{11}(\alpha_n - 2\beta_n + 1) < \frac{7}{11}(\alpha_n - 2\beta_n + 1)$$

（由于当 $n \geqslant 2$ 时，$\beta_n \geqslant 2 > \frac{16}{11}$）

综合以上两种情况的讨论，由数学归纳法就证明了引理。

引理 13.3.23 设 γ 表示一个正奇数，h, k 都是自然数，那么不定方程

$$\frac{3^h\gamma - 1}{2^h\gamma - 1} = 2^k$$

的唯一正整数解为 $\gamma = h = k = 1$。

证明 设 $h > 1$，则由 α_h, k_h 的定义知 $2^{h+k_h} < 3^h < 2^{h+k_h+1}$，因而

$$2^{k_h} < \left(\frac{3}{2}\right)^h < 2^{k_h+1}$$

又由引理 13.3.22 知对一切 $h > 1$，成立 $u_n < a_h - 2\beta_h + 1$，或者

$$3^h - 2^{h+k_h} < 2^{h+k_h} - 2 \cdot 2^{k_h} + 1$$

由此得出
$$\frac{3^h - 1}{2^h - 1} < 2^{k_h+1}$$

因而有
$$2^{k_h} < \left(\frac{3}{2}\right)^h < \frac{3^h y - 1}{2^h y - 1} \leqslant \frac{3^h - 1}{2^h - 1} < 2^{k_h+1}$$

这就证明了当 $h > 1$ 时，$\frac{3^h y - 1}{2^h y - 1}$ 不可能是 2 的整数幂，因而$\frac{3^h y - 1}{2^h y - 1} = 2^k$ 无解。

当 $h = 1$ 时，只有当 $y = 1$ 时，$\frac{3y - 1}{2y - 1} = 2^1$ 是正整数解。故$\frac{3^h y - 1}{2^h y - 1} = 2^k$ 的唯一正整数解就是 $y = h = k = 1$。

下面给出 $3x + 1$ 映射的周期解存在的一个必要条件。

引理 13.3.24 设 x 是一个正奇数，$x_1 = x, x_2 = T(x_1), \cdots, x_m = T(x_{m-1})$。如果 $x_m = x_1$ 是 $3x + 1$ 映射的周期解，则 x_m 必具有形式 $x_m = B^{k_n} C^{h_n} B^{k_{n-1}} C^{h_{n-1}} \cdots B^{k_1} C^{h_1}(x)$，其中 $h_1, k_1, h_2, k_2, \cdots, h_n, k_n$ 都是自然数。

证明 由引理 13.3.12 知 x_m 只可能有两种形式，即

$$x_m = C^{h_n} B^{k_{n-1}} C^{h_{n-1}} \cdots B^{k_1} C^{h_1}(x)$$

或
$$x_m = B^{k_n} C^{h_n} B^{k_{n-1}} C^{h_{n-1}} \cdots B^{k_1} C^{h_1}(x)$$

假设 $x_m = C^{h_n} B^{k_{n-1}} C^{h_{n-1}} \cdots B^{k_1} C^{h_1}(x)$ 或 $x_m = C^{h_n}(x_{n-1})$，那么由引理 13.3.13 可知必存在着正的奇数 y_1, y_n 使得

$$x_1 = 2^{h_1} y_1 - 1, x_m = 3^{h_n} y_n - 1$$

这时由于 x_1 是奇数，而 x_m 是偶数，因此不可能成立 $x_m = x_1$，这就证明了引理。

定理 13.3.1 $3x + 1$ 映射的 $B^k C^h x = x$ 类型的周期解的唯一解是平凡解 $x = h = k = 1$，其中 x 是一个正奇数。

证明 根据映射 B, C 的定义，x 是一个正奇数，因此 x 必可写成 $x = 2^n y - 1$ 的形式。从引理 13.3.11 和 $B^k C^h x = x$ 可知，必有 $n = h$(由于 $x = 2^n y - 1$，那么 x 恰可被算子 C 作用 n 次，$C^n x = 3^n - 1$ 已成为一个偶数，因此 $C^n x$ 不可能再被算子 C 作用，而只能被算子 B 作用，因而 x 的轨道具有形式 $\cdots B^{k_1} C^n x$。如果 $n \neq h$，则 x 的轨道形式与假设矛盾。因此必有 $n = h$，同理可证必有 $k_1 = k$)。因而由 $B^k C^h x = x$ 得出

$$B^k C^h x = \frac{3^h y - 1}{2^k} = x = 2^h y - 1$$

或
$$\frac{3^h y - 1}{2^h y - 1} = 2^k$$

由引理 13.3.23 知上述方程的唯一正整数解为 $y = h = k = 1$，由此就得出$3x + 1$ 映射的 $B^k C^h x = x$ 类型的周期解的唯一解为 $x = h = k = 1$，即平凡解。

从上面的讨论看出，$3x+1$映射的周期解和不定方程有着密切的联系。下面我们说明，$3x+1$问题的一般解也和不定方程有着密切的联系。

定义 13.3.7 设x是一个使得$3x+1$猜想成立的正奇数，即存在一个自然数n，使得

$$T^n x = 1$$

则称x是一个$3x+1$数。

引理 13.3.25 x是一个$3x+1$数的必要条件是可以表示成以下形式

$$x=\frac{1}{3^n}(2^{m_1+m_2+\cdots+m_n}-2^{m_1+\cdots+m_{n-1}}-2^{m_1+\cdots+m_{n-2}}\cdot 3-\cdots-2^{m_1}\cdot 3^{n-2}-3^{n-1})$$

证明 由$3x+1$数的定义知存在奇自然数$x_1=x,x_2,\cdots,x_n$及自然数m_1，$m_2,\cdots,m_n$使得

$$3x_1+1=2^{m_1}x_2$$
$$3x_2+1=2^{m_2}x_3$$
$$\vdots$$
$$3x_n+1=2^{m_n}$$

于是

$$x_n=\frac{1}{3}(2^{m_n}-1)$$

$$x_{n-1}=\frac{1}{3}(2^{m_{n-1}}x_n-1)=\frac{1}{3^2}(2^{m_{n-1}+m_n}-2^{m_{n-1}}-3)$$

$$\vdots$$

$$x=x_1=\frac{1}{3^n}(2^{m_1+m_2+\cdots+m_n}-2^{m_1+\cdots+m_{n-1}}-2^{m_1+\cdots+m_{n-2}}\cdot 3-\cdots-2^{m_1}\cdot 3^{n-2}-3^{n-1})$$

但是要注意$3x+1$数的这种表示方法不是唯一的。例如

$$1=\frac{1}{3^n}(2^{2+2+\cdots+2}-2^{2+\cdots+2}-2^{2+\cdots+2}\cdot 3-\cdots-2^2\cdot 3^{n-2}-3^{n-1})$$

(上式中从左数起，2的幂中分别含有$n,n-1,\cdots,2$个2)

下面证明，除了上述循环外，$3x+1$数可以唯一地表示为引理13.3.25中的形式。

引理 13.3.26 设x是一个大于1的$3x+1$数，则存在着都大于1的奇自然数$x_1=x,x_2,\cdots,x_n$和自然数$m_1,m_2,\cdots,m_n$(其中m_n是不小于4的偶数)，使得

$$3x_1+1=2^{m_1}x_2$$
$$3x_2+1=2^{m_2}x_3$$
$$\vdots$$
$$3x_n+1=2^{m_n}$$

$$x = \frac{1}{3^n}(2^{m_1+m_2+\cdots+m_n} - 2^{m_1+\cdots+m_{n-1}} - 2^{m_1+\cdots+m_{n-2}} \cdot 3 - \cdots - 2^{m_1} \cdot 3^{n-2} - 3^{n-1})$$

证明 在引理13.3.25的证明中可设 $x_1, x_2, \cdots, x_n$ 都不等于1。如果 m_n 是奇数，则 $m_n = 2q + 1, q \geqslant 0$。当 $q \geqslant 1$ 时

$$2^{m_n} - 1 = 2^{2q+1} - 1 = 2 \cdot 4^q - 1 \equiv 2 \cdot 1 - 1 \pmod 3 \equiv 1 \pmod 3$$

与

$$3x_{n+1} = 2^{m_n} \Rightarrow 2^{m_n} - 1 \equiv 0 \pmod 3$$

矛盾，$q = 0 \Rightarrow m_n = 1$ 也得出一个矛盾 $3x_n + 1 = 2$，因此 m_n 必须是偶数。从 $x_n \neq 1$ 及 $3x_n + 1 = 2^{m_n}$ 知必有 $m_n \geqslant 4$。

引理13.3.27 设 x 是一个大于1的 $3x+1$ 数，则引理13.3.26中的奇自然数 $x_1 = x, x_2, \cdots, x_n (x_1, x_2, \cdots, x_n > 1)$，及自然数 $m_1, m_2, \cdots, m_n (m_n \geqslant 4, m_n$ 是偶数) 被 x 唯一地确定。

证明 假设存在着两组自然数 $m_1, m_2, \cdots, m_p (m_p \geqslant 4, m_p$ 是偶数)，$n_1, n_2, \cdots, n_p (n_p \geqslant 4, n_p$ 是偶数)，及两组大于1的奇数 $y_1 = x, y_2, \cdots, y_p, z_1 = x, z_2, \cdots, z_p$，使得引理13.3.28成立。如果 $p \neq q$，则不妨设 $q > p$。那么由

$$3x + 1 = 2^{m_1} y_2 = 2^{n_1} z_2 \Rightarrow m_1 = n_1, y_2 = z_2 = x_2$$

$$3x_2 + 1 = 2^{m_2} y_3 = 2^{n_2} z_3 \Rightarrow m_2 = n_2, y_3 = z_3 = x_3$$

$$\vdots$$

$$3x_p + 1 = 2^{m_p} = 2^{n_p} z_{p+1} \Rightarrow m_p = n_p, z_{p+1} = 1$$

这与 $z_{p+1} > 1$ 矛盾。故必有 $p = q, m_i = n_i, y_i = z_i, 1 \leqslant i \leqslant p$。

引理13.3.28 设 x 是大于1的奇数，且存在着自然数 $m_1, m_2, \cdots, m_n (m_n \geqslant 4, m_n$ 是偶数) 使得

$$x = \frac{1}{3^n}(2^{m_1+m_2+\cdots+m_n} - 2^{m_1+\cdots+m_{n-1}} - 2^{m_1+\cdots+m_{n-2}} \cdot 3 - \cdots - 2^{m_1} \cdot 3^{n-2} - 3^{n-1})$$

则 x 必是一个 $3x+1$ 数，且必存在着都大于1的奇数 $x_1 = x, x_2, \cdots, x_n$ 使得

$$3x_1 + 1 = 2^{m_1} x_2$$

$$3x_2 + 1 = 2^{m_2} x_3$$

$$\vdots$$

$$3x_n + 1 = 2^{m_n}$$

证明 令 $M_k = \sum_{i=1}^{k} m_i$，则

$$x = \frac{1}{3^n}(2^{M_n} - 2^{M_{n-1}} - 2^{M_{n-2}} \cdot 3 - \cdots - 2^{M_1} \cdot 3^{n-2} - 3^{n-1}) =$$

$$\frac{1}{3^n}(2^{M_{n-1}}(2^{m_n} - 1) - 2^{M_{n-2}} \cdot 3 - \cdots - 2^{M_1} \cdot 3^{n-2} - 3^{n-1})$$

因为 $m_n \geqslant 4$ 是偶数，故 $3 \mid 2^{m_n} - 1$，从而存在大于1的奇数 $x_n = \frac{1}{3}(2^{m_n} - 1)$，

由此可得

$$x = \frac{1}{3^n}(2^{M_{n-1}}3x_n - 2^{M_{n-2}}\cdot 3 - \cdots - 2^{M_1}\cdot 3^{n-2} - 3^{n-1}) =$$

$$\frac{1}{3^{n-1}}(2^{M_{n-1}}x_n - 2^{M_{n-2}} - 2^{M_{n-3}}\cdot 3 - \cdots - 2^{M_1}\cdot 3^{n-3} - 3^{n-2}) =$$

$$\frac{1}{3^{n-1}}(2^{M_{n-2}}(2^{m_{n-1}}x_n - 1) - 2^{M_{n-3}}\cdot 3 - \cdots - 2^{M_1}\cdot 3^{n-3} - 3^{n-2})$$

如果 $3\nmid 2^{M_{n-1}}x_n - 1$,则 x 不可能是整数,与假设矛盾,故 $x_{n-1} = \frac{2^{m_{n-1}}x_n - 1}{3}$ 是整数,因而是奇数。如果 $x_{n-1} = 1$,那么由

$$\frac{2^{m_{n-1}}x_n - 1}{3} = 1 \Rightarrow m_{n-1} = 2, x_n = 1$$

与 $x_n > 1$ 矛盾。因此必有 $x_{n-1} > 1$。同理可得

$$x_{n-2} = \frac{2^{m_{n-2}}x_{n-1} - 1}{3}, \cdots, x_2 = \frac{2^{m_2}x_3 - 1}{3}, x_1 = \frac{2^{m_1}x_2 - 1}{3}$$

都是大于 1 的奇数。由 $x_1 = x, x_2, \cdots, x_n$ 的定义可以看出它们显然满足方程组

$$\begin{gathered}3x_1 + 1 = 2^{m_1}x_2\\ 3x_2 + 1 = 2^{m_2}x_3\\ \vdots\\ 3x_n + 1 = 2^{m_n}\end{gathered}$$

因而 x 是一个 $3x+1$ 数。

由引理 13.3.26 ~ 引理 13.3.28 即可得出

定理 13.3.2　大于 1 的奇数 x 是 $3x+1$ 数的充分必要条件是 x 可以表为

$$x = \frac{1}{3^n}(2^{m_1+m_2+\cdots+m_n} - 2^{m_1+\cdots+m_{n-1}} - 2^{m_1+\cdots+m_{n-2}}\cdot 3 - \cdots - 2^{m_1}\cdot 3^{n-2} - 3^{n-1})$$

的形式,其中 $m_1, m_2, \cdots, m_n$ 是自然数,且 $m_n \geqslant 4$ 是偶数。如果 x 具有上述表示,则这一表示是唯一的,即表示式中的 $m_1, m_2, \cdots, m_n$ 被 x 唯一地确定。

定理 13.3.3　设 $x_1 = x, x_2, \cdots, x_n$ 都是大于 1 的奇数,$m_1, m_2, \cdots, m_n$ 是自然数,且 $m_n \geqslant 4$ 是偶数,则不定方程组

$$\begin{gathered}3x_1 + 1 = 2^{m_1}x_2\\ 3x_2 + 1 = 2^{m_2}x_3\\ \vdots\\ 3x_n + 1 = 2^{m_n}\end{gathered}$$

或不定方程

$$x = \frac{1}{3^n}(2^{m_1+m_2+\cdots+m_n} - 2^{m_1+\cdots+m_{n-1}} - 2^{m_1+\cdots+m_{n-2}}\cdot 3 - \cdots - 2^{m_1}\cdot 3^{n-2} - 3^{n-1})$$

有唯一解的充分必要条件是 x 是 $3x+1$ 数。

给表达式 $x=\frac{1}{3^n}(2^{m_1+m_2+\cdots+m_n}-2^{m_1+\cdots+m_{n-1}}-2^{m_1+\cdots+m_{n-2}}\cdot 3-\cdots-2^{m_1}\cdot 3^{n-2}-3^{n-1})$ 中的 $m_1,m_2,\cdots,m_n$ 以各种特殊值，则当 x 是一个奇自然数时就可以得出各种 $3x+1$ 数，其中的 n 称为 x 的维数。例如，令 $n=1$，则当 $\frac{1}{3}(2^{2m_1}-1)=\frac{4^{m_1}-1}{3}$ 是一个奇自然数时，就可得出所有一维的 $3x+1$ 数：5,21,85,…。实际上容易证明对任何自然数 m_1，$\frac{4^{m_1}-1}{3}$ 的确表示一个奇自然数。令 $n=2$，则当 $\frac{1}{9}(2^{m_1+m_2}-2^{m_2}-3)$ 是一个奇自然数时，就可得出所有的二维的 $3x+1$ 数。（见表 13.3.1，其中的 × 号表示 m_1,m_2 对应的表示式 $\frac{1}{9}(2^{m_1+m_2}-2^{m_2}-3)$ 不是一个奇数的情况。）

表 13.3.1　二维的 $3x+1$ 数

m_1 \ m_2	4	6	8	10	12	…
1	3	×	×	227	×	…
2	×	×	113	×	×	…
3	13	×	×	909	×	…
4	×	×	453	×	×	…
5	53	×	×	3 637	×	…
…	…	…	…	…	…	…

实际上可以证明当 $m_2\equiv 0 \pmod 6$ 时，$\frac{1}{9}(2^{m_1+m_2}-2^{m_2}-3)$ 不是一个自然数，当 $m_1\equiv 1 \pmod 2, m_2\equiv 4 \pmod 6$ 或 $m_1\equiv 0 \pmod 2, m_2\equiv 2 \pmod 6$ 时，$\frac{1}{9}(2^{m_1+m_2}-2^{m_2}-3)$ 的确是一个奇自然数。

最后再介绍一个与 $3x+1$ 猜想有关的猜想，称为弱 $3x+1$ 猜想。

弱 $3x+1$ 猜想：设 $G=\left\{\frac{2n+1}{3n+2}\middle| n\geqslant 0\right\}\cup\{2\}$，$S$ 是由 G 中有限个元素的乘积组成的集合（或者说，G 是 S 的乘法生成集），则 S 包含所有的自然数。

可以证明，由 $3x+1$ 猜想可以推出弱 $3x+1$ 猜想。

习题 13.3

1.(1) 如果 k 是一个使得 $k \equiv 5 \pmod 8$ 的奇自然数，则存在奇自然数 $k_1 < k$，使得 $k = 4k_1 + 1$；

(2) 如果 k_1, k_2 都是奇自然数，使得 $k_2 = 4k_1 + 1$，则 k_1, k_2 中必有一个数（记为 k）使得 $k \equiv 5 \pmod 8$。

2. 设 k 是一个奇自然数，n 是自然数，$m = 4^n k + 4^{n-1} + \cdots + 4 + 1$，则 $m \equiv 5 \pmod 8$。

3. 设 k 是一个奇自然数，n 是自然数，$m = 4^n k + 4^{n-1} + \cdots + 4 + 1$，，那么如果

(1) $k \equiv 1 \pmod 6$ 且 $n \equiv 2 \pmod 3$ 或

(2) $k \equiv 3 \pmod 6$ 且 $n \equiv 0 \pmod 3$ 或

(3) $k \equiv 5 \pmod 6$ 且 $n \equiv 1 \pmod 3$。

则 $m \equiv 3 \pmod 6$。

4. 设 T 表示 $3x + 1$ 映射，$m_k = T^k m$，则 $m_k \not\equiv 3 \pmod 6$。

5. 设 k 是一个奇自然数，$k \not\equiv 3 \pmod 6$，则存在奇自然数 $m \equiv 3 \pmod 6$ 和自然数 n 使得 $T^n m = k$。

6. 证明：当 $n > 1$ 时，$(2^n - 1) \nmid (3^n - 1)$。

7. 证明：$3x + 1$ 猜想蕴含弱 $3x + 1$ 猜想。

参 考 文 献

[1] 伽莫夫 G.从1到无穷大——科学中的事实和臆测[M].修订版.北京:科学出版社,2002年.
[2] 别尔曼 Γ H.数与数的科学[M].上海:商务印书馆,1957.
[3] 亚历山大洛夫 A Д,等.数学——他的内容、方法和意义.第一卷[M].北京:科学普及出版社,1958.
[4] 亚历山大洛夫 A Д,等.数学——他的内容、方法和意义.第二卷[M].北京:科学普及出版社,1959.
[5] 亚历山大洛夫 A Д,等.数学——他的内容、方法和意义.第三卷[M].北京:科学普及出版社,1962.
[6] 克莱因 M.古今数学思想.第1册[M].上海:上海科学技术出版社,1979.
[7] 克莱因 M.古今数学思想.第2册[M].上海:上海科学技术出版社,1979.
[8] 克莱因 M.古今数学思想.第3册[M].上海:上海科学技术出版社,1980.
[9] 克莱因 M.古今数学思想.第4册[M].上海:上海科学技术出版社,1980.
[10] 柯朗 R,罗宾斯 H.数学是什么[M].长沙:湖南教育出版社,1985.
[11] 徐莼舫.中国算术故事[M].北京:中国青年出版社,1965.
[12] 徐莼舫.中国代数故事[M].北京:中国青年出版社,1965.
[13] 徐莼舫.古算趣味[M].北京:中国青年出版社,1962.
[14] 查有梁,等.杰出数学家秦九韶[M].北京:科学出版社,2003.
[15] 菲赫金哥尔茨 Γ M.微积分学教程(修订本).第一卷.第一分册[M].北京:人民教育出版社,1959.
[16] 菲赫金哥尔茨 Γ M.微积分学教程(修订本).第一卷.第二分册[M].北京:人民教育出版社,1959.
[17] 菲赫金哥尔茨 Γ M.微积分学教程.第二卷.第一分册[M].北京:人民教育出版社,1956.
[18] 菲赫金哥尔茨 Γ M.微积分学教程.第二卷.第二分册[M].北京:人民教育出版社,1954.
[19] 菲赫金哥尔茨 Γ M.微积分学教程.第二卷.第三分册[M].北京:人民教育出版社,1954.
[20] 菲赫金哥尔茨 Γ M.微积分学教程.第三卷.第一分册[M].北京:人民教

育出版社,1957.
[21] 菲赫金哥尔茨 Γ M.微积分学教程.第三卷.第二分册[M]. 北京:人民教育出版社,1957.
[22] 菲赫金哥尔茨 Γ M.微积分学教程.第三卷.第三分册[M]. 北京:人民教育出版社,1955.
[23] 那汤松 И П.实变函数论(修订本).上册[M]. 北京:高等教育出版社,1958.
[24] 那汤松 И П.实变函数论(修订本).下册[M]. 北京:高等教育出版社,1958.
[25] 黄国勋,李炯生.计数[M]. 上海:上海教育出版社,1983.
[26] 王子侠,单墫.对应[M]. 北京:科学技术文献出版社,1989.
[27] 单墫.集合及其子集[M]. 上海:上海教育出版社,2001.
[28] 闵嗣鹤,严士健.初等数论[M].2 版. 北京:人民教育出版社,1982.
[29] 华罗庚.数论导引[M]. 北京:科学出版社,1957.
[30] 维诺格拉多夫 И M.数论基础(修订本)[M]. 北京:高等教育出版社,1956.
[31] 苏什凯维奇 A K.数论初等教程[M]. 北京:高等教育出版社,1956.
[32] 杜德利 U.基础数论[M]. 上海:上海科学技术出版社,1980.
[33] 余红兵.数学竞赛中的数论问题[M]. 北京:中国少年儿童出版社.1992.
[34] 柯召,孙琦.初等数论 100 例[M]. 上海:上海教育出版社,1980.
[35] 潘承洞,于秀源.阶的估计[M]. 济南:山东科学技术出版社,1983.
[36] 潘承洞,潘承彪.素数定理的初等证明[M]. 上海:上海科学技术出版社,1983.
[37] 潘承洞,潘承彪.初等数论[M]. 北京:北京大学出版社,1992.
[38] 潘承洞,潘承彪.初等代数数论[M]. 济南:山东大学出版社,1991.
[39] 潘承彪.解析数论基础[M]. 北京:科学出版社,1997.
[40] KNUTH D E.计算机程序设计艺术.第一卷 基本算法[M].3 版. 北京:国防工业出版社,2002.
[41] RAMANUJICHARY K. Number Theory with computer applications, Prentice-Hall [M]. New Jersey: Upper saddle Rever, 1998.
[42] POLLARD H.代数数论[M]. 台北:徐氏基金会,1973.
[43] APOSTOL T M. Modular Functions and Dirichlet Series in Number Theory[M]. New York: Inc Springer-Verlag, 1976.
[44] 周民强.实变函数论[M].2 版. 北京:北京大学出版社,1995.
[45] 李元中,常心怡. 实变函数论[M]. 西安:陕西师范大学出版社,1989.

[46] 江泽坚,吴智泉.实变函数论[M]. 北京:人民教育出版社,1961.
[47] 夏道行,等.实变函数论与泛函分析.上册[M]. 北京:人民教育出版社,1978.
[48] 夏道行,等.实变函数论与泛函分析.下册[M]. 北京:人民教育出版社,1979.
[49] 吉米多维奇 Б П.数学分析习题集(修订本)[M]. 北京:人民教育出版社,1958.
[50] 林源渠,方企勤,李正元,等.数学分析习题集[M]. 北京:高等教育出版社,1986.
[51] 裴礼文.数学分析中的典型问题与方法[M]. 北京:高等教育出版社,1993.
[52] 宋国柱.分析中的基本定理和典型方法[M]. 北京:科学出版社,2004.
[53] 谢惠民,等.数学分析习题课讲义.上册[M]. 北京:高等教育出版社,2003.
[54] 谢惠民,等.数学分析习题课讲义.下册[M]. 北京:高等教育出版社,2004.
[55] 肖振纲.移数问题——循环小数的一个应用[M]//数学竞赛(16).长沙:湖南教育出版社,1992.
[56] 辛钦 A Я.连分数[M]. 上海:上海科学技术出版社,1965.
[57] 朱尧辰,王连祥.丢番图逼近引论[M]. 北京:科学出版社,1993.
[58] 奥尔德斯 C D.连分数[M]. 北京:北京大学出版社,1985.
[59] 朱尧辰,徐广善.超越数引论[M]. 北京:科学出版社,2003.
[60] CASSELS J W S. An Introduction to diophantine approximation [M]. london : Cambridge University Press,1957.
[61] KUIPCRS L, NIEDERREITE H. Uniform distribution of sequences[EB]. John Wiley & Sons, 1974.
[62] NIVEN. Irrational Numbers[EB]. Rahway New Jersey: J. Wiley and Sons Inc, 1956.
[63] 北京大学数学力学系几何与代数教研室代数小组.高等代数讲义[M]. 北京:高等教育出版社,1965.
[64] 熊全淹.近世代数[M].2 版. 上海:上海科学技术出版社,1978.
[65] 张广祥.抽象代数——理论、问题与方法[M]. 北京:科学出版社,2005.
[66] BARBEAU E J. Polynomials[M]. New York Inc: Springer-Verlag, 1989.
[67] BORWEIN P, ERDELYI T. Polynomials and Polynomial Inequalities. 北京,广州,上海,西安:Springer-Verlag,世界图书出版公司,1995.

[68] 常庚哲.复数计算与几何证题[M]. 上海:上海教育出版社,1980.

[69] 蒋声.从单位根谈起[M]. 上海:上海教育出版社,1980.

[70] 安德鲁,皮克林.实践的冲撞——时间,力量与科学[M]. 南京:南京大学出版社,2004.

[71] 楼世拓,邬冬华.黎曼猜想[M]. 沈阳:辽宁教育出版社,1987.

[72] 库洛什 А Г.高等代数教程[M]. 北京:商务印书馆,1953.

[73] 法捷耶夫 Д К,索明斯基 И С.高等代数习题集[M].2 版. 北京:高等教育出版社,1987.

[74] 张禾瑞,郝炳新.高等代数[M]. 北京:高等教育出版社,1960.

[75] 周伯壎.高等代数[M]. 北京:高等教育出版社,1966.

[76] 魏壁.方程式[M]. 北京:中国青年出版社,1962.

[77] 尤秉礼.常微分方程补充教程[M]. 北京:人民教育出版社,1981.

[78] HARDY G H, WRIGHT E M. An Introduction to the Theory of Numbers (fifth edition). Oxford, London, Glasgow: The English language book society and Oxford University Press, 1981.

[79] EDWARDS H M. Fermat's Last Theorem, A Genetic Introduction to Algebraic Number Theory. Heidelberg Berlin: Springer-Verlag, 1977.

[80] 北京大学《计算方法》编写组.计算方法.上册[M]. 北京:科学出版社,1975.

[81] 北京大学《计算方法》编写组.计算方法.下册[M]. 北京:科学出版社,1980.

[82] 卢侃,孙建华,欧阳容百,等.混沌动力学[M]. 上海:上海翻译出版社,1990.

[83] 丁玖,周爱辉.确定性系统的统计性质[M]. 北京:清华大学出版社,2006.

[84] FENG BEIYE. Periodic traveling-wave solution of Brusselator[J]. ACTA. Appl. Math. Sinica, 1988,4(4):324-332.

[85] 陈文成,陈国良.Hopf 分支的代数判据[J].应用数学学报,1992,15(4):251-259.

[86] FENG BEIYE. An simple elementary proof for the inequality d _ n < 3^n[J]. Acta Mathematicae Applicatae Sinica, English Series, 2005, 21(3):455-458;

[87] 冯贝叶.四次函数实零点的完全判据和正定条件[J].应用数学学报,2006,29(3):454-466.

[88] 朱照宣.谈抛物线[J].数学教学,1983,3(3):3-7.

[89] SAHA P, STROGATZ S H. The Birth of Period Three [J]. Mathematics Magazine, 1995, 68(1):42-47.

[90] BECHHOEFER J. The Birth of Period 3, Revisited, Mathematics Magazine [J]. 1996, 69(2): 115-118.

[91] GORDON W B. Period Three Trajectories of the Logisitic Map [J]. Mathematics Magazine, 1996, 69(2): 118-120.

[92] BURM J. P Fishback, Period-3 Orbits via Sylvester's Theorem and Resultants [J]. Mathematics Magazine, 2001, 74(1): 47-51.

[93] WANG JINGLONG. A Property on Irrational Number [J]. 华东师范大学学报(自然科学版), 1999, 2: 36-40.

[94] HUYLEBROUCK D. Similarities in Irrationality Proofs for π, ln 2, ζ(2), and ζ(3)[J]. The American Mathematical Monthly, 2001, 108: 222-231.

[95] LAGARIAS J C. The $3x+1$ Problem and Its Generalizations [J]. The American Mathematical Monthly, 1985, 92 (3): 3-23.

[96] LAGARIAS J C. Wild and Wooley Numbers [J]. The American Mathematical Monthly, 2006, 113: 97-08.

[97] BOROS G, MOLL V. Irresistible Integrals[M]. Cambridge: Cambridge University Press, 2004.

[98] VAKIL R. A Mathematical Mosaic[M]. Burlington: Brendan Kelly Publishing Inc, 1996.

冯贝叶发表论文专著一览

一、论文

[L1] 冯贝叶,钱敏.分界线环的稳定性及其分支出极限环的条件.数学学报,1985,28(1):53-70.

[L2] FENG BEIYE. Condition of creation of limit cycle from the loop of a saddle- point separatrix. ACTA. Math. Sinica(N.S),1987,3(4):55-70.

[L3] FENG BEIYE. Periodic traveling-wave solution of Brusselator. ACTA. Appl. Math. Sinica,1988,4(4):324-332.

[L4] FENG BEIYE. Bifurcation of limit cycles from a center in the two-parameter system. ACTA. Appl. Math. Sinica,1990,6(1):44-49.

[L5] 冯贝叶.临界情况下奇环的稳定性.数学学报,1990,33(1):113-134.

[L6] 冯贝叶.临界情况下 Heteroclinic 环的稳定性.中国科学,1991,7A:673-684.

[L7] FENG BEIYE. The stability of a heteroclinic cycle for the critical case. Sciences in China,1991,34(8):920-934.

[L8] 冯贝叶,肖冬梅.奇环的奇环分支.数学学报,1992,35(6):815-830.

[L9] 冯贝叶.无穷远分界线环的 Melnikov 判据及二次系统极限环的分布.应用数学学报, 1993,16(4):482-492.

[L10] 冯贝叶.关于"三微弱同宿吸引子的判别准则"一文的反例.科学通报,1994,39(2):187.

[L11] 冯贝叶.同宿及异宿轨线的研究近况.数学研究与评论,1994,14(2):299-311.

[L12] 冯贝叶.无穷远分界线的稳定性和产生极限环的条件.数学学报,1995,38(5):682-695.

[L13] 冯贝叶.空间同宿环和异宿环的稳定性.数学学报,1996,39(5):649-658.

[L14] FENG BEIYE. The heteroclinic cycle in the model of competition between n species and its stability. ACTA. Appl. Math. Sinica,1998,14(4):404-413.

[L15] 冯贝叶.关于多项式系统的一个公开问题的解答.应用数学学报,2000,23(2):314-315.

[L16] 冯贝叶,胡锐.具有两点异宿环的二次系统.应用数学学报,2001,24(4):481-486.

[L17] 冯贝叶,曾宪武.蛙卵有丝分裂模型的定性分析.应用数学学报,2002,25(3):460-468.

[L18] FENG BEIYE, ZHENG ZUOHUAN. Periodic Solution of a Simplified Model of Mitosis in Frog Eggs. ACTA. Appl. Math. Sinica,2002,18(4):625-628.

[L19] FENG BEIYE, HU RUI. A Survey On Homoclinic And Heteroclinic Orbits, Applied Mathematics E-Notes,2003(3),16-37.

[L20] LIU SHIDA, FU ZUNTAO, LIU SHIKUO, XIN GUOJUN, LIANG FU MING and FENG BEIYE. Solitary Wave in Linear ODE with Variable Coefficients, Commun. Theor. Phys. (Beijing, China),2003(39):643-846.

[L21] 冯贝叶.蛙卵有丝分裂模型的鞍结点不变圈及其分支.应用数学学报,2004,27(1):36-43.

[L22] LIU ZHICONG, FENG BEIYE. Qualitative Analysis For A Class Of Plane Systems. Applied Mathematics E-Notes,2004,(4)74-79.

[L23] LIU ZHICONG, FENG BEIYE. Qualitative Analysis For Rheodynamic Model of Cardiac Pressure Pulsations. ACTA. Appl. Math. Sinica,2004,20(4):573-578.

[L24] 胡锐,冯贝叶.推广后继函数法研究第二临界情况下同宿环的稳定性.应用数学学报,2005,28(1):28-43.

[L25] FENG BEIYE. An simple elementary proof for the inequality d-n < 3^n, Acta Mathematicae Applicatae Sinica, English Series,2005,21(3):455-458.

[L26] 冯贝叶.四次函数实零点的完全判据和正定条件.应用数学学报,2006,29(3):454-466.

二、专著

[Z1] 李继彬,冯贝叶.稳定性、分支与混沌.昆明:云南科技出版社,1995.

[Z2] 张锦炎,冯贝叶.常微分方程几何理论与分支问题(第二次修订本).北京:北京大学出版社,2000.

三、科普作品及译作校对

[K1] 冯贝叶.一个中学生的札记.数学通报,1965(9):25-26.

[K2] 冯贝叶.神奇的魔方,一点不假.数学译林,2000,19(2):157-161.

[K3] 冯贝叶.15方块游戏的现代处理.数学译林,2000,19(2):162-168.

[K4] 冯贝叶.第五十九届 William Lowell Putnan 数学竞赛.数学译林,2000,19(2):152-156.

[K5] 冯贝叶.不动点和费马定理:处理数论问题的一种动力系统方法.数学译林,2000,19(4):339-345.

[K6] 冯贝叶.A.N.科尔莫果罗夫(Kolmogorov).数学译林,2001,20(1):67-75.

[K7] 冯贝叶.π, ln 2, $\zeta(2)$, $\zeta(3)$的无理性证明中的类似性.数学译林,2001,20(3):256-265.

(以上有些译文发表时用了徐秀兰等名字)

◎编辑手记

一、关于书稿

如果说淘书是一种乐趣，著书是一种态度，藏书是一种品味，读书是一种生活，那么出版书就是一种眼光。

冯贝叶先生的这部巨著不是我策划的，但是我发现的，窃以为编辑的核心能力是鉴赏力，即独到的眼光，久浸书海，这方面我有相当的自信。

发行经理张荣一天告诉我说有人在网上征求书稿出版，遂要来资料一看是冯先生之女冯南南所为。

对冯先生久闻大名，上世纪90年代初非线性科学在中国开始流行，哈尔滨虽地处边陲，但也组织了一个民间的非线性沙龙，吸引了数学、哲学、计算机、经济学等学科的诸多青年学子。本人也“混迹”其中（只是资质平庸，没能修成正果），在小组当时收集的文献中便有冯先生和张锦炎先生的大作《常微分方程几何理论与分支问题》，所以有仰慕之情。待书稿传来，通读后才知冯先生居然还是初等数论爱好者。偶翻刚刚寄到的《数学通报》2007年第11期上有一篇我国著名数理逻辑学家王世强先生的文章《本刊读者对于“一组有趣的数学”的回应》，其中特别提到了两位热心读者就是冯先生及其女冯南南．给人感觉冯先生即居“庙堂”之高在《中国科学》上发表大文章也涉“江湖”之远，与业余人士共探初数之趣（许多数学大家视初等数论为雕虫小技）。初等数论乃我至爱，故又生同好之喜。二者相加遂决定冒效益不佳之风险，高调推出，并为此仿德国 Springer 出版社的一套丛书，将其定为 HIT 数学·统计学系列丛书之第一本。

二、关于书名

为了应付变幻莫测的图书市场，我开始想将书名定为《从希帕索斯到胡尔维茨》，因为之前我们的一本《从毕达哥拉斯到怀尔斯》已获市场认可。但冯先生表示反对，说有哗众取宠之嫌，还应老老实实叫《多项式和无理数》，尽管我已经征求多位数学同行意见，均表示这个书名过于平淡，但恭敬不如从命(在与数学大家或老年人有异议时，妥协的往往是编辑)，我希望最后由市场来说服冯先生而不是由我，职业数学家做逻辑推理多年，总是精显执著有余，妥协不足，不过从理论上说冯先生书名起得是有典可据的。1956年高等教育出版社就出版了N·B·勃罗斯库列亚柯夫著的《数与多项式》(译者是我国著名数学家吴品三，印数是令现在每个策划编辑向往的14 000册，而定价则是每个现在读者所怀念的1.10元)，勃罗斯库列亚柯夫在1948年10月25日所写的序中说："数和多项式，初看来，彼此是不同的，但是有很多共同点。它们都定义有同样性质的加减乘除的运算，并且都是近世代数基本概念之一环的特殊情形。因此，有可能在一种共同理论的范围内来研究数和多项式。"及至近年高等教育出版社与斯普林格出版社又联合出版了冯克勤与余红兵两位教授合写的《整数与多项式》。在序言中也强调了相同的观点，所以此书名倒是中规中矩。

三、关于内容

冯先生的大作中除少量"原创"内容外，其余均为用自己的理解详细表述已有结果，此书特别适合自学看，但我担心现在诺大中国还有自学数学之人了吗?(想当年《数理化自学丛书》举国瞩目，一书难求)，所以此书优点是细(对自学者)，但缺点是太细(对购买者，因为篇幅长，定价自然高)。

法国著名数学家埃利·嘉当(Elie Cartan)1940年2月27日在前南斯拉夫贝尔格莱德的法国研究院所作的演讲中指出："数学和其他科学一样，存在着两类科学家：第一类通过提出新想法开辟康庄大道，这些想法通常简单但未被他人发现；第二类则在第一类为了到达他们自己的花园而清除过的辽阔土地上劳作，经常可以摘到可口的果实，而且有时还能获得巨大的收获。"数学图书的作者同样也有两类：一类是风景园艺建筑师式的人物，他们只写属于自己的创作，另外一类是导游式的人物，他带领游人欣赏第一类人建筑的美景，按嘉当的话说，虽然"前者更应该被人们记住和授予荣誉，但后者不仅仅是重要的那么简单，应该是不可或缺的"。冯先生二者兼而有之，其份量相信读者读完之后自有评价。

另外在稿件加工过程中冯先生的认真与严谨给我们留下深刻印象，向冯先生学习。

策划编辑　刘培杰

2007年12月15日